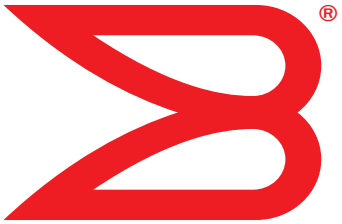
53-1001778-01
30 March 2010



Brocade SMI Agent

User's Guide

Supporting SMI Agent 120.11.0

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Brocade SMI Agent User’s Guide	53-1000109-01	New document.	April 2006
Brocade SMI Agent User’s Guide	53-1000199-01	Updated to support Fabric OS 5.2.0 and SMI-A 110.5.0.	November 2006
Brocade SMI Agent User’s Guide	53-1000199-02	Rebranded the document using the new Brocade templates.	March 2007
Brocade SMI Agent User’s Guide	53-1000446-01	Updated to support Fabric OS 5.3.0 and SMI-A 120.6.0	June 2007
Brocade SMI Agent User’s Guide	53-1000613-01	Updated to support Fabric OS 6.0.0 and SMI-A 120.7.0.	November 2007
Brocade SMI Agent User’s Guide	53-1000613-02	Updated to support Fabric OS 6.1.0 and SMI-A 120.7.1.	March 2008
Brocade SMI Agent User’s Guide	53-1001146-01	Updated to support Fabric OS 6.1.1 and SMI-A 120.7.2	August 2008

Title	Publication number	Summary of changes	Date
Brocade SMI Agent User's Guide	53-1001199-01	Updated to support Fabric OS 6.2.0 and SMI-A 120.8.0	December 2008
Brocade SMI Agent User's Guide	53-1001199-02	Minor corrections to the previous version.	February 2009
Brocade SMI Agent User's Guide	53-1001263-01	Updated to support Fabric OS 6.1.2_cee and SMI-A 120.9.0	March 2009
Brocade SMI Agent User's Guide	53-1001263-02	Updated the procedure for adding proxy connections.	April 2009
Brocade SMI Agent User's Guide	53-1001263-03	Updated the Brocade logo.	July 2009
Brocade SMI Agent User's Guide	53-1001535-01	Updated to support Fabric OS 6.3.0 and SMI-A 120.10.0.	August 2009
Brocade SMI Agent User's Guide	53-1001778-01	Updated to support Fabric OS 6.4.0 and SMI-A 120.11.0.	March 2010

Contents

About This Document

In this chapter

How this document is organized

This document is a user's guide written for end users to help you learn about starting, stopping, and configuring the Brocade SMI Agent.

This document is organized to help you find the particular information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Overview," provides an overview of the CIM, the Brocade SMI-S initiative, and the Brocade SMI Agent.
- Chapter 2, "Brocade SMI Agent," explains how to start and stop the Brocade SMI Agent.
- Chapter 3, "Brocade SMI Agent Configuration," describes how to use the Brocade SMI Agent Configuration Tool for configuring SMI-A settings, such as fabric proxy connections, agent security, port settings, and logging options.
- Chapter 4, "Mutual Authentication for Clients and Indications," explains how to enable mutual authentication for clients and indications manually, after installation.
- Chapter 5, "Frequently Asked Questions," provides answers to the most frequently asked questions sent to the SMI Agent Developer Support e-mail address.
- Appendix A, "Licenses and Attributions," includes the licenses for open source software.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for SMI-A 120.11.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Brocade SMI Agent 120.11.0:

- Brocade 200E switch
- Brocade 300 switch
- Brocade 3000 switch
- Brocade 3014 switch
- Brocade 3016 switch
- Brocade 3200 switch
- Brocade 3250 switch
- Brocade 3600 switch
- Brocade 3800 switch
- Brocade 3850 switch
- Brocade 3900 switch
- Brocade 4012 switch
- Brocade 4016 switch
- Brocade 4018 switch
- Brocade 4020 switch
- Brocade 4024 switch
- Brocade 4100 switch
- Brocade 4424 switch
- Brocade 4900 switch
- Brocade 5000 switch
- Brocade 5100 switch
- Brocade 5300 switch
- Brocade 5410 switch
- Brocade M5424 switch
- Brocade 5460 switch
- Brocade 5470 switch
- Brocade 5480 switch
- Brocade 7500 Extension Switch
- Brocade 7500E Extension Switch
- Brocade 7600 Application Appliance
- Brocade 7800 Extension Switch

- Brocade 8000 Application Appliance
- Brocade 8470 switch
- Brocade VA-40FC switch
- Brocade 12000 director (only on Fabric OS 5.0.x)
- Brocade 24000 director (single domain only)
- Brocade 48000 director
- Brocade Encryption Switch
- Brocade Multiprotocol Router Model AP7420 (only as a non-proxy switch)
- Brocade DCX Data Center Backbone
- Brocade DCX-4S Data Center Backbone
- The following blades are supported on the Brocade DCX and DCX-4S:
  - Port blades: FC8-16, FC8-32, FC8-48, FC8-64
  - FC4 port blades
  - FC10-6
  - FC4-16IP
  - FC4-48C
  - FCoE10-24
  - FA4-18
  - FR4-18i
  - FS8-18
  - FX8-24

What's new in this document

- New hardware platform supported (Brocade 8470)
- New blade supported (FC8-64)

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command and method names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI

italic text	Provides emphasis Identifies variables Identifies class properties Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on Brocade Connect. See "Brocade resources" on page xiii for instructions on accessing Brocade Connect.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
IBM Corporation	AIX
Linus Torvalds	Linux
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Novell, Inc.	SUSE

Corporation	Referenced Trademarks and Products
Sun Microsystems, Inc.	Sun, Solaris
Red Hat, Inc.	Red Hat, Red Hat Network
VMware, Inc.	VMware

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

The following SMI-A documentation can be obtained from developer support at Brocade:

- *Brocade SMI Agent Installation Guide*
- *Brocade SMI Agent Developer's Guide*

To get up-to-the-minute information, go to *http://my.brocade.com* and register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

For additional Brocade documentation, visit the Brocade Web site:

http://www.brocade.com

Release notes are available on the My Brocade web site and are also bundled with the Fabric OS firmware.

Other industry resources

For information about the Distributed Management Task Force (DMTF), including information about CIM standards and educational materials:

http://www.dmtf.org

For information about the Storage Management Initiative (SMI) of the Storage Networking Industry Association (SNIA), including the Storage Management Initiative Specification (SMI-S):

http://www.snia.org/smi/home

For information about Web Based Enterprise Management (WBEM):

http://wbemservices.sourceforge.net/

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
   - Switch model
   - Switch operating system version
   - Software name and software version, if applicable
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
2. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.:

   The serial number label is located as follows:

   - *Brocade 200E*—On the nonport side of the chassis
   - *Brocade 300, 4100, 4900, 5100, 5300, 7500, 7500E, 7800, 8000, VA-40FC,* and *Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - *Brocade 3014*—On the top of the chassis, under the insertion arm
   - *Brocade 3016 and 4012*—On the bottom of the switch module
   - *Brocade 3250, 3850, and 7600*—On the bottom of the chassis
   - *Brocade 3900*— Nonport side of the chassis
   - *Brocade 4016*—On the top of the switch module
   - *Brocade 4018*—On the top of the blade
   - *Brocade 4020 and 4024*—On the bottom of the switch module
   - *Brocade 5000*—On the switch ID pull-out tab located on the bottom of the port side of the switch

- *Brocade 8470*—On the top of the chassis
- *Brocade 12000, 24000, and 48000*—Inside the chassis next to the power supply bays
- *Brocade DCX*—On the bottom right on the port side of the chassis
- Brocade DCX-4S—On the bottom right on the port side of the chassis, directly above the cable management comb.
- *Brocade Multiprotocol Router Model AP7420*—On the bottom of the chassis and on the back of the chassis.

1. World Wide Name (WWN)

   Use the **licenseIdShow** command to display the WWN of the chassis.

   If you cannot use the **licenseIdShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

   For the Brocade Multiprotocol Router Model AP7420: Provide the switch WWN. Use the **switchShow** command to display the switch WWN.

Brocade SMI Agent support

Report any problems or issues in using the Brocade SMI Agent to the following e-mail address:

support@brocade.com

When contacting support at Brocade, provide the following:

- Operating system version and patch level
- Sample code exhibiting problem (if possible)
- Switch models and operating system versions, including the proxy switch
- Compiler version
- Error messages received
- XML received from the Brocade SMI Agent
- XML sent to the Brocade SMI Agent
- Steps followed to produce the problem
- Server-side console output and log files
- Thread dump, if the SMI Agent is hanging or if memory consumption goes up

You can use the SMI Agent Configuration Tool, which is described in this document, to collect the required support information to be sent.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1

Overview

In this chapter

Common Information Model (CIM)

The Common Information Model (CIM) is a conceptual, object-based information model defined by the Distributed Management Task Force (DMTF) for describing management, which is not bound to a particular implementation. This allows for the interchange of management information between management systems and applications.

CIM consists of two parts:

- CIM Specification
- CIM Schema

The CIM Specification describes the language, naming, metaschema, and mapping techniques to other management models, such as SNMP MIBs and FC-GS. The metaschema is a formal definition of the model that defines the terms used to express the model and their usage and semantics. The elements of the metaschema are *classes*, *properties*, and *methods*. The metaschema also supports *indications* and *associations* as types of classes and *references* as types of properties.

The CIM Schema provides the actual model descriptions. The CIM Schema supplies a set of classes with properties and associations that provide a well-understood conceptual framework within which it is possible to organize the available information about the managed environment. The CIM Schema itself is structured into three distinct layers:

- Core Schema
- Common Schema
- Extension Schema

The *Core Schema* defines basic classes, such as a managed element or an association. The *Common Schema* provides a set of foundation classes that can be used as the super-class to describe other devices, such as a system, a device, or a network. The *Extension Schema* allows users to expand the definitions in the Common Schema to describe specific device types, such as a Brocade FC switch.

The formal definition of the CIM Schema is expressed in a managed object format (MOF) file, which is an ASCII file that can be used as input into a MOF editor, parser, or compiler to generate code for use in a provider or client application.

Web-Based Enterprise Management (WBEM) is a set of management and internet standard technologies to unify management of an enterprise. It includes CIM, CIM Schemas, CIM operations over HTTP, and CIM-XML encoding.

Brocade SMI-S Initiative

Storage Management Initiative (SMI) is a broad-based initiative sponsored by the Storage Networking Industry Association (SNIA) that is standardizing all aspects of storage management for multivendor storage networking products. SMI encompasses the storage aspects of CIM, as shown in Figure 1.

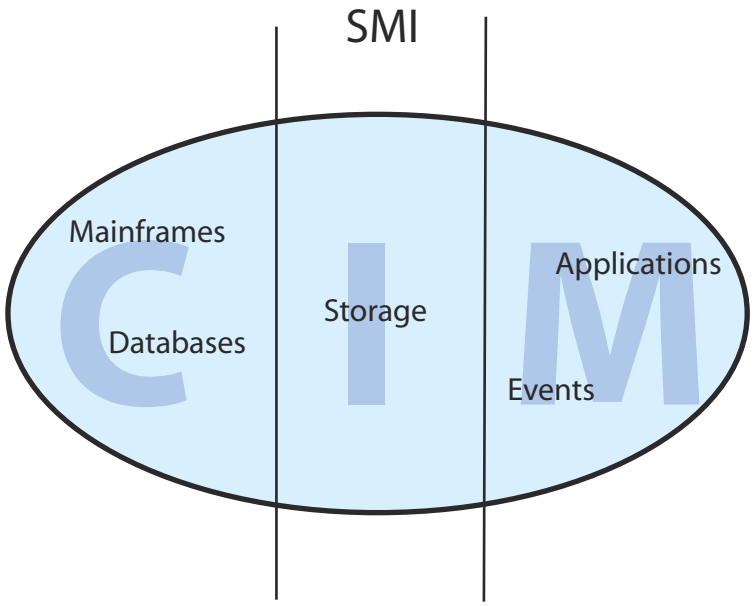


FIGURE 1 Storage Management Initiative

The Storage Management Initiative Specification (SMI-S) defines the interface that allows storage management systems to manage and monitor storage area network (SAN) resources.

SMI-S is the only standard that addresses manageability from the perspective of a logical unit number (LUN) in a storage array, all the way through the data path, to an application running on a host. The standard promises to remove much of the vendor-specific issues associated with managing storage, storage networks, hosts, and applications by providing a common interface and management paradigm across the full scope of application and storage management. This in turn will improve the interoperability of various management products and allow more products to be managed by most management environments. Customers will benefit from a much wider choice of broad-based management applications.

Brocade SMI Agent

The Brocade SMI Agent (SMI-A) is a “proxy” agent to multiple fabrics; it resides on a separate host. The SMI-A does not require any modification or upgrade to deployed fabrics when it is deployed. All the support required in Brocade switches is already in place. Figure 2 on page 3 shows the high-level architecture of the SMI-A.

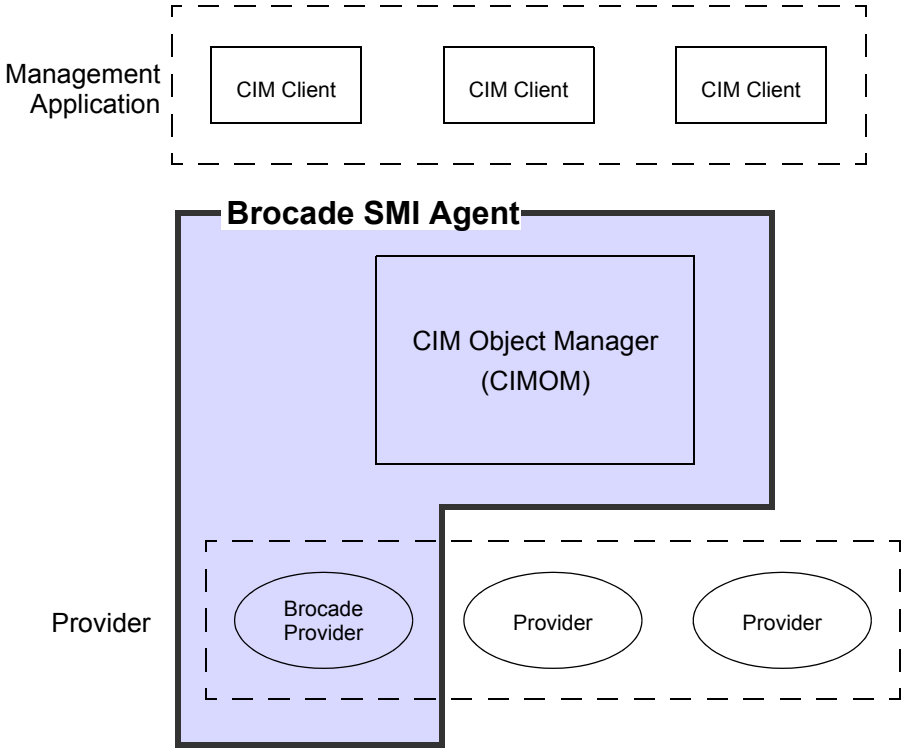


FIGURE 2 Brocade SMI Agent high-level architecture

The Brocade SMI Agent supports the evolving SMI-S standard and the Brocade functionality not available through the standard.

The Brocade SMI Agent provides the following features:

- CIM agent compliant with SMI-S, with support for the following profiles:
  - Server profile (supported by the SMI-A with CIMOM vendor-supplied providers)
  - Fabric profile
  - Switch profile
  - Extender profile (discovery only)
  - FC HBA profile

  The *Brocade SMI Agent Developer's Guide* has additional information about the supported profiles and subprofiles.
- Additional support for physical objects such as chassis, blades, fans, power supplies, temperature sensors, and transceivers
- Support for the following:
  - Connection and account management
  - Port performance and error statistics
  - HBA and device information via FDMI
  - Configuration download to switches
  - Firmware download to switches

  - SLP (Service Location Protocol) to discover SMI-S profiles
  - CIM agent management using CIM
  - Indications: life-cycle indications for fabrics, SANs, nodes, switches, and switch ports; and alert indications for many fabric events.
  - Basic support for non-Brocade switches (switches, ports, topology information, and so on)
  - HTTP and HTTPS protocols
  - HTTP and HTTPS port configuration
  - Mutual authentication for clients and indications
  - Security authorization using native OS access control mechanisms
  - Provider logging of exceptions, operations, and performance metrics for diagnostic purposes
  - Secure SAN fabrics
  - Secure RPC communication
  - CIM queries, using WBEM Query Language (WQL)
- DMTF CIM Schema v2.19 (final)

Chapter

Brocade SMI Agent

2

In this chapter

Start the Brocade SMI Agent

There are two ways you can start the SMI-A:

- from the command line
- as a service or daemon

You can start the SMI-A as a service only if the option to start as a service was selected during installation or if you configure the SMI-A as a service using the Brocade SMI-A Configuration Tool, as described in "SMI Agent service configuration and removal" on page 31.

The following procedures describe how to start the SMI-A without security and with security enabled.

By default, security is disabled on all platforms. In this case, *security* is the authentication of the client username and password (and domain name, if security is enabled on Windows by selecting domain authentication) when connecting to the server. The procedure for enabling security varies, depending on the platform.

On Solaris, Linux, or AIX, if security is enabled for the SMI-A, start the SMI-A as a root using the *start_server* script.

NOTE
This document uses <*SMIAgent*> to refer to the installation folder, although your installation folder might be different (if you changed it from the default).

Starting the SMI-A

1. Type the following at the command line:

   On Linux, Solaris, and AIX:

   sh <*SMIAgent*>**/agent/server/jserver/bin/start_server.sh**

On Windows:

<*SMIAgent*>**\agent\server\jserver\bin\start_server.bat**

On Windows, you can also click **Start > Programs >** *SMIAgent* **> Start CIMOM**.

The SMI-A is now ready to use.

Starting the SMI-A as a service

1. Type the following at the command line:

   On Linux, Solaris, and AIX:

   sh <*SMIAgent*>**/agent/server/jserver/bin/start_agent_service.sh**

   On Windows:

   <*SMIAgent*>**\agent\server\jserver\bin\start_agent_service.bat**

   On Windows, you can also click **Start > Programs >** *SMIAgent* **> Start SMI Agent Service**.

Stop the Brocade SMI Agent

To stop the SMI-A, refer to the following procedures. If mutual authentication for clients is enabled and the HTTP service is disabled, use the procedure "Stopping the SMI-A when mutual authentication for clients is enabled".

If the SLP daemon was started, stop the daemon using the procedures described in "Service Location Protocol (SLP) support" on page 7.

NOTE

On Linux, Solaris, or AIX, if security is enabled for the agent, then the **stop_server** or **stop_agent_service** command should be provided with a username and password. For example:

```
sh <SMIAgent>/agent/server/jserver/bin/stop_server.sh -s
http://localhost:<portnum>/interop -u <username> -p <password>
```

Stopping the SMI-A

1. Select one of the following options depending on your operating system:

   a. On Windows, select **Start > Programs >** *SMIAgent* **> Stop CIMOM**.

      1. Alternatively, you can open a command prompt that is different from the window in which the *start_server.bat* file is running.
      2. Run the following:

         <*SMIAgent*>**/agent/server/jserver/bin/stop_server.bat**

   a. On Linux, Solaris, or AIX, become the root user: for example, % su root.

      Run the following:

      ```
      sh <SMIAgent>/agent/server/jserver/bin/stop_server.sh
      -s http://localhost:portnum/interop
      ```

      The protocol, host, and port information are required only when the defaults are changed.

Stopping the SMI-A when mutual authentication for clients is enabled

1. Modify the stop_server script to specify the CLASSPATH for the *WbemClient.properties* file. (See "Client configuration to use client certificates" on page 48 if the *WbemClient.properties* file is not used.)

   The CLASSPATH should contain only the path to the directory where the file is present and not the path to the file itself. For example, if the *WbemClient.properties* file is located at *C:\SMIAgent\agent*, then the CLASSPATH should be:

   C:\SMIAgent\agent

2. Run the following command to stop the SMI-A:

   ```
   <SMIAgent>/agent/server/jserver/bin/stop_server
   -s https://localhost:<HTTPSPort>/interop
   ```

   This command is the same on all platforms. The protocol, host, and port information are required only when the defaults are changed.

Stopping the SMI-A as a service

1. Type the following at the command line:

   On Linux, Solaris, and AIX:

   ```
   sh <SMIAgent>/agent/server/jserver/bin/stop_agent_service.sh
   -s http://localhost:<portnum>/interop
   ```

   On Windows:

   ```
   <SMIAgent>\agent\server\jserver\bin\stop_agent_service.bat
   ```

   On Windows, you can also click **Start > Programs >** *SMIAgent* **> Stop SMI Agent Service**.

Service Location Protocol (SLP) support

The Brocade SMI Agent supports SLP to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

A WBEM client is not required to use SLP discovery to find a WBEM Server; that is, it might already know about the location and capabilities of the WBEM Server to which it wants to send its requests. In such environments, starting the SLP component of the SMI-A is not needed.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, the SLP component of the SMI-A should be started to allow advertisement of its existence, location, and capabilities.

NOTE
If you want SLP support, you must install and start the SLP daemon prior to starting the SMI-A.

Brocade SMI Agent SLP support consists of the following components:

- slpd script that starts up the slpd platform-specific program
- slpd program that acts as a Service Agent (SA). A different slpd binary executable exists for Solaris, Linux, AIX, and Windows.

- slptool script that starts up the slptool platform-specific program
- slptool program that can be used to verify that SLP is operating properly. A different slptool exists for Solaris, Linux, AIX, and Windows.

By default, the SMI-A is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show that the SMI-A:

- accepts WBEM requests over HTTP without SSL on TCP port 5988
- accepts WBEM requests over HTTPS using SSL on TCP port 5989

slptool commands

Although the IP address shown below might vary, the following slptool commands can be used to verify that the SLP is operating properly:

- slptool findsrvs service:service-agent

  This command verifies that the SMI-A SLP service is properly running as a Service Agent (SA). Although the IP address might be different, it should produce output similar to the following:

  ```
  service:service-agent://127.0.0.1,65535
  ```

- slptool findsrvs service:wbem

  This command verifies that the SMI-A SLP service is properly advertising its WBEM services. Although the IP address might be different, it should produce output similar to the following:

  ```
  service:wbem:https://10.0.1.3:5989,65535
  service:wbem:http://10.0.1.3:5988,65535
  ```

  This output shows that the SMI-A:

  - accepts WBEM requests over HTTP using SSL on TCP port 5989
  - accepts WBEM requests over HTTP without SSL on TCP port 5988

- slptool findattrs service:wbem:http://10.0.1.2:5988

  This command verifies that the SMI-A SLP service is properly advertising its WBEM SLP template over the HTTP protocol. Note: Change the IP Address:Port to those displayed by slptool findsrvs service:wbem.

- slptool findattrs service:wbem:https://10.0.1.2:5989

  This command verifies that the SMI-A SLP service is properly advertising its WBEM SLP template over the HTTPS protocol.

NOTE
Change the IP Address:Port to those displayed by slptool findsrvs service:wbem.

SLP on Linux, Solaris, and AIX

On Linux, Solaris, and AIX, you do not need to install the SLP service.

Starting SLP on Linux, Solaris, and AIX

1. Become the root user:

   ```
   % su root
   ```

2. Check that the SLP daemon is not already started:

   ```
   # ps -eaf | grep slpd
   ```

3. Start the SLP daemon, if one is not already started:

   ```
   # <SMIAgent>/agent/bin/slpd
   ```

Stopping SLP on Linux, Solaris, and AIX

1. Become the root user:

   ```
   % su root
   ```

2. Find the process ID for the SLP daemon:

   ```
   # ps -eaf | grep slpd
   ```

3. Stop the SLP daemon process, if found:

   ```
   # kill -9 <slp_process_id>
   ```

An SLP log file can be found at:

<SMIAgent>/agent/cfg/slp.log

The SLP daemon can be reconfigured by modifying the following file:

<SMIAgent>/agent/cfg/slp.conf

Applications that do not dynamically register themselves with SLP using SLPAPIs can instead register statically by modifying the following file:

<SMIAgent>/agent/cfg/slp.reg

For more information about these files, read the comments contained in them, or read:

http://www.openslp.org/doc/html/UsersGuide/index.html

Verifying that the SLP service is correctly installed and operating

1. Become the root user:

   ```
   % su root
   ```

2. Verify that the SLP service is properly running as a Service Agent (SA):

   ```
   # <SMIAgent>/agent/bin/slptool findsrvs service:service-agent
   ```

3. Verify that the SLP service is properly advertising its WBEM services:

   ```
   # <SMIAgent>/agent/bin/slptool findsrvs service:wbem
   ```

4. Verify that the SLP service is properly advertising the WBEM SLP template over its configured client protocol adapters.

NOTE
Change the IP Address:Port to those displayed by slptool findsrvs service:wbem:

```
# <SMIAgent>/agent/bin/slptool findattrs
service:wbem:http://192.168.0.100:5988

# <SMIAgent>/agent/bin/slptool findattrs
service:wbem:https://192.168.0.100:5989
```

SLP on Windows

This section describes how to install, start, and verify the SLP daemon on Windows.

On Windows, the SLP service must be installed from a command prompt. It need only be installed once, but must be installed before starting the SMI-A.

Installing SLP on Windows

1. Open a command prompt via **Start > Programs > Accessories > Command Prompt**.
2. Change to the directory where *slpd.bat* is located:

   cd C:*<SMIAgent>***\agent\bin**
3. Run **slpd -install** to install the SLP service into Windows. If SLP is already installed, the following message displays:

   ```
   CreateService failed - The specified service already exists. (0x431)
   ```

Starting SLP on Windows

1. Install the SLP service, as described in "Installing SLP on Windows".
2. Open a command prompt via **Start > Programs > Accessories > Command Prompt**.
3. Change to the directory where *slpd.bat* is located:

   cd C:*<SMIAgent>***\agent\bin**
4. Run **slpd -start** to start the SLP service.

   You can also start the SLP service from the Windows Service Console. If the SLP is installed as a Windows service, you should access the Services Console and ensure that the startup is set to Automatic.

An SLP log file can be found at:

<SMIAgent>\agent\cfg\slp.log

The SLP daemon can be reconfigured by modifying the following file:

<SMIAgent>\agent\cfg\slp.conf

Applications that do not dynamically register themselves with SLP using SLPAPIs can instead be statically registered by modifying the following file:

<SMIAgent>\agent\cfg\slp.reg

For more information about these files, read the comments contained in them or read:

http://www.openslp.org/doc/html/UsersGuide/index.html

Verifying that the SLP service is correctly installed and operating

1. Start the SLP service and SMI-A.
2. Open a command prompt via **Start > Programs > Accessories > Command Prompt**.
3. Change to the directory where *slpd.bat* is located:

   cd C:<*SMIAgent*>**\agent\bin**
4. Verify that the SLP service is properly running as a Service Agent.

   > **slptool findsrvs service:service-agent**
5. Verify that the SLP service is properly advertising its WBEM services:

   > **slptool findsrvs service:wbem**
6. Verify that the SLP service is properly advertising its WBEM SLP template over its configured Client Protocol Adapters. Note: Change the IP Address:Port to those displayed by slptool findsrvs service:wbem

   > **slptool findattrs service:wbem:http://192.168.0.100:5988**
   > **slptool findattrs service:wbem:https://192.168.0.100:5989**

Disable HTTP for security reasons

If security or mutual authentication is enabled, you might want to disable the unsecure HTTP protocol, leaving only the secure HTTPS enabled. There are two ways to enable and disable the HTTP protocol:

- Use the SMI-A Configuration Tool (see "Configuring HTTP access" on page 24).
- Use the command-line scripts packaged by the SMI-A installer.

  The SMI-A installer packages the scripts DeleteXMLProtocolAdapter to permanently disable the HTTP port used by the SMI-A and CreateXMLProtocolAdapter to enable the HTTP port again. These scripts can be found in the following directory:

  <SMIAgent>/agent/bin

Connection monitoring

The SMI-A handles connection monitoring for the connection to the proxy switch. Whenever there is a connection failure to the proxy switch, by default the SMI-A automatically tries to reconnect to the proxy switch 5 times with a wait time of 90 seconds between each retry. This process is repeated every 30 minutes until the connection is reestablished to the proxy switch.

NOTE
The actual time between each retry is the 90-second wait time plus the retry time (the time spent on reestablishing the connection to the proxy switch). The retry time is beyond the SMI Agent's control.

These default values of 5 retries, 90-second sleep interval between retries, and 30 minutes between each retry process are all configurable through the Brocade_ConnectionMonitoringService and through instances of Brocade_ConnectionMonitor. These values are not configurable through the SMI-A installer or configuration tool.

Enable multi-homed support

The Brocade SMI Agent supports multi-homed hosts; that is, hosts configured with multiple IPs. This means that you can configure which IP address the SMI Agent should use for Event and ARR registration on the switch.

Configuring IP address for switch-to-SMIAgent communication in multi-homed systems

1. Edit the *SMIAgentConfig.xml* file found at *.../server/jserver/bin* with the following entry:

   ```
   <host address="xxx.xxx.xxx.xxx"/>
   ```

   For example,

   ```
   <?xml version="1.0" encoding="ISO-8859-1"?>
   <!DOCTYPE agent_config SYSTEM "SMIAgentConfig.dtd">
   <agent_config>
   <dbserver driver="" is_password_encrypted="" password="" url=""
   username=""/>
   <port_config arr="5400" eventing="123"/>
   <secureport_config arr="876" eventing="1"/>
   <host address="10.201.64.173"/>
   </agent_config>
   ```

2. Restart the Brocade SMI Agent.

Configuring IP address for SMI Agent client to server communication in multi-homed systems

1. Edit the *jserver.properties* file found at *...server/jserver/bin* with the following entry:

   ```
   HostIPAddress=xxx.xxx.xxx.xxx
   ```

2. Restart the Brocade SMI Agent.

Chapter

Brocade SMI Agent Configuration

3

In this chapter

About the Brocade SMI Agent Configuration Tool

The Brocade SMI Agent Configuration Tool is a graphical interface for configuring SMI-A settings, such as fabric proxy connections, agent security, port settings, and logging options. This tool is installed during SMI-A installation and can be used after installation is complete.

You must install the Brocade SMI Agent before you can use the Configuration Tool. The Configuration Tool is automatically installed as part of the SMI-A installation.

This chapter describes how to use the tool to make configuration changes *after* installation, without re-running the installation wizard.

The Brocade SMI Agent Configuration Tool consists of several components, illustrated in Figure 3 on page 14.

- Title bar

  The title bar displays the version of the SMI Agent.

- Menu tree

  The menu tree displays the actions you can perform using the Configuration Tool. You can expand or collapse the tree to display various groups of commands. By default, the tree is fully expanded.

- Content pane

  The content pane displays information relevant to the command that is selected in the menu tree and provides options to configure the functionalities provided by the command.

- Server buttons

  Some of the commands require you to start or stop the SMI-A server before they take effect. Use the **Start Server** and **Stop Server** buttons to start and stop the SMI-A server. If the SMI-A is configured as a service, the **Start Server** and **Stop Server** buttons start and stop the SMI-A as a service.

  These buttons also show the current status of the SMI-A server. If the server is running, the **Start Server** button is disabled; if the server is *not* running, the **Stop Server** button is disabled.

- Action buttons

  Apply — Applies the changes you have made in the content pane, without closing the window.

  Cancel — Cancels the changes you have made in the content pane, without closing the window. Already applied changes cannot be undone.

  Exit — Closes the window and exits the application. You are prompted to apply any unsaved changes.

NOTE
If user authentication is enabled, you are required to provide your user name and password in a dialog box prior to performing certain actions (such as starting or stopping the server).

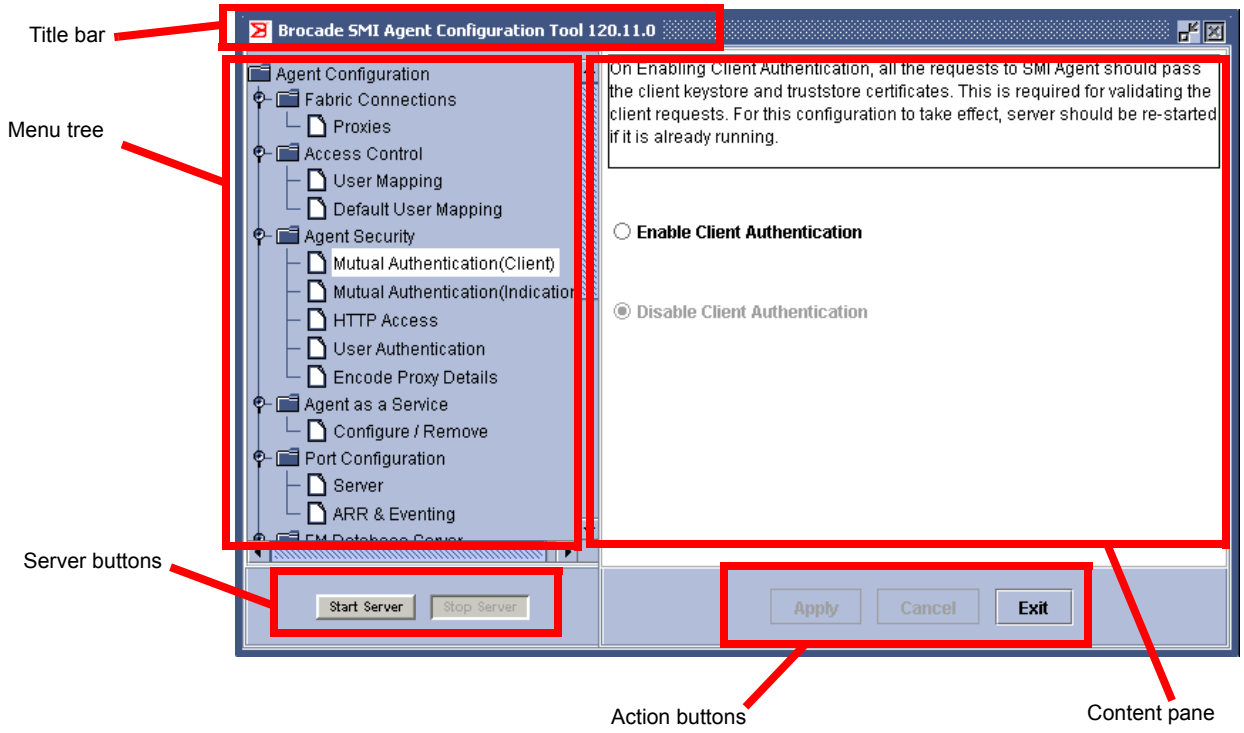


FIGURE 3 Components of the Brocade SMI Agent Configuration Tool

Launch the Brocade SMI-A Configuration Tool

Because this is a graphical tool, for Linux, Solaris, and AIX, you must be on a console with an XWindows Manager or, if you are working remotely, export the display.

Launching the Brocade SMI Agent Configuration Tool (Linux, Solaris, and AIX)

1. Navigate to the directory where the tool is located.

   <SMIAgent>/agent/server/jserver/bin

   where <SMIAgent> is the directory where the Brocade SMI Agent is installed.

2. Execute the following command:

   ./configurationtool.sh

   The Brocade SMI Agent Configuration Tool launches, as shown in Figure 4.

Launching the Brocade SMI Agent Configuration Tool (Windows)

- Click **Start > Programs >** *SMIAgent* **> Brocade SMI Agent Configuration Tool**.

  The Brocade SMI Agent Configuration Tool launches, as shown in Figure 4.

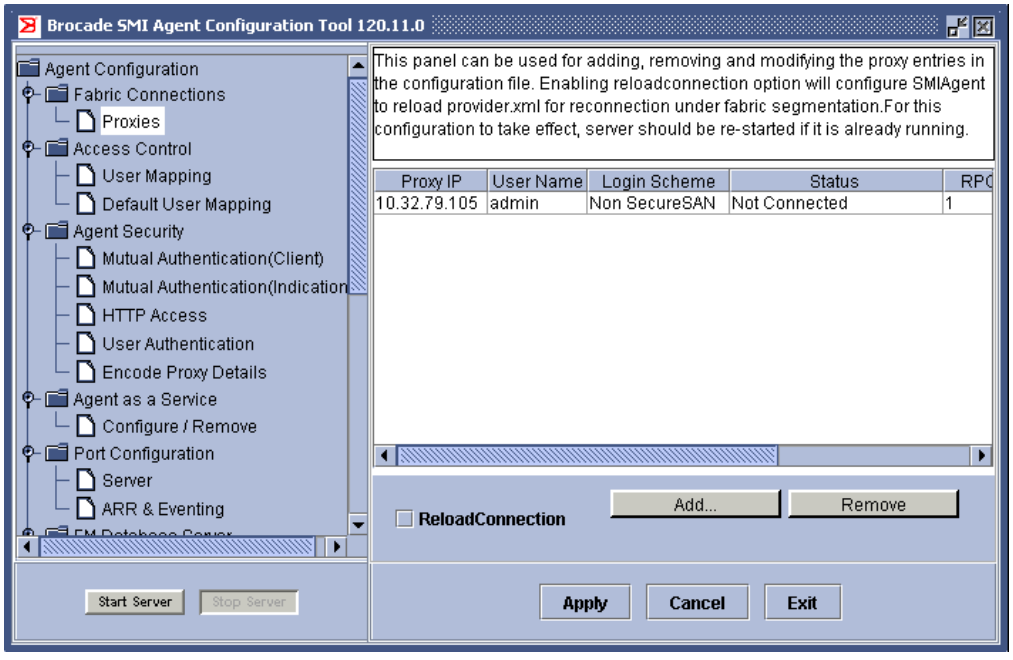


FIGURE 4 Brocade SMI Agent Configuration Tool

Proxy connections

The SMI-A installation wizard automatically configures the *provider.xml* file with the fabric information that is added during the installation process. This section describes how you can add or remove proxy entries manually after installation is done.

You can also choose to have the SMI-A attempt to reload the provider.xml when fabric segmentation occurs.

When you add proxy entries, the SMI-A attempts to log in to every one. If you have proxy entries for different switches in the same fabric, the SMI-A establishes only one connection to the fabric, using the first valid switch in the list. Subsequent login attempts to the same fabric result in an informative error message: “A duplicate switch in the fabric has been identified and will be removed.”

By default, passwords are stored in encrypted format in the *provider.xml* file. Duplicate proxy IP addresses are not allowed.

The *provider.xml* file is located in the <*SMIAgent*>*agent**server**jserver**bin* directory.

Reloading provider.xml on fabric segmentation

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Proxies** in the menu tree (see Figure 4 on page 15).
3. Select the **ReloadConnection** check box.
4. Click **Apply**.

Including multiple switch connection entries from the same fabric in the provider.xml

1. Stop the SMIA server.
2. Edit the *provider.xml* manually as mentioned above by providing the connection entry for each switch.
3. Enable the connection reload through the Configuration Tool.

   Alternatively, you can edit the *SMIAgentConfig.xml* and set the connection reload flag to true so that rescan of the *provider.xml* is enabled.
4. Start the SMIA server.

Adding proxy connections

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Proxies** in the menu tree (see Figure 4 on page 15).
3. Click **Add**.
4. Fill out the **Proxy Configuration** dialog box (see Figure 5) and click **OK**.

The configuration values for the new fabric are displayed in the content pane. The value in the Status column is **Not Connected**, which means that the proxy entry is configured but the SMI-A is not connected to the fabric.

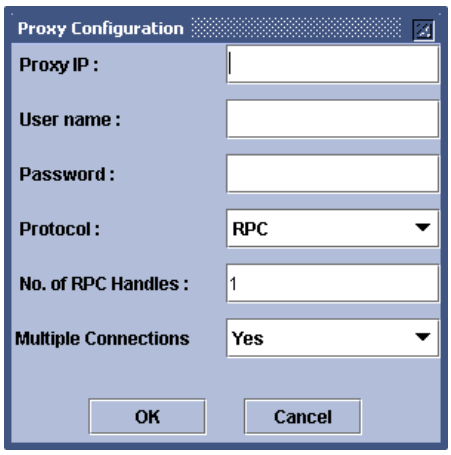


FIGURE 5 **Proxy Configuration dialog box**

5. Click **Apply**.

   You are prompted to start the SMI-A if it is not already started. Click **Start Server** in the lower left corner of the window.

   The SMI-A attempts to log in to the fabric. The **Status** field in the content pane displays the status of the login attempt. When login is successful, the **Status** field displays **Connected**.

NOTE
The proxy that is added during installation cannot be removed from the Brocade SMI Agent Configuration Tool if the status is “Login Failed”.

Removing proxy connections

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Proxies** in the menu tree (see Figure 4 on page 15).
3. Select the proxy in the content pane and click **Remove**.

   The value in the **Status** column for this fabric changes to **Marked for Delete**, which means that the proxy entry is configured but the SMI-A is not connected to the fabric.
4. Click **Apply**.

   The SMI-A attempts to log out of the fabric. If the logout is successful, the proxy entry is removed from the content pane.

Login failure status information

If the login fails, the SMI-A displays a message in the Status column of the Proxies panel (see Figure 4 on page 15). You can see the full message as a tool tip or by expanding the Status column. Table 1 lists the status messages and corresponding descriptions, as well as the return code from the **LoginAsUser** extrinsic method.

TABLE 1 Login failure status messages

LoginAsUser Return Code	Status message in Proxies panel	Description
RT_NOT_SUPPORTED	Not supported	Access protocol is not supported.
RT_ALREADY_EXISTS	Duplicate Connection	Attempt to make an additional connection to an already connected switch, or an attempt to make a connection to a switch in a fabric that is already connected through another switch.
RT_PWD_EXPIRED	Password Expired	Login failed due to password expired.
RT_ACCOUNT_LOCKOUT	Account Lockout	Login account is locked out.
RT_ACCOUNT_DISABLED	Account Disabled	Login account is disabled.
RT_TIMEOUT	Connection Timed Out	Connection timed out.
RT_FAILED	Connection Failed	
RT_SUCCESS	Connected	Login successful.
RT_INVALID_PARAMETER	Invalid Connection Parameter	Some connection parameters are invalid.
RT_INSUFFICIENT_VF_ MEMBERSHIP	Insufficient VF Membership	Login failed due to insufficient VF (user does not have admin/chassis access across VF) membership.
RT_INSUFFICIENT_USER_ROLE	Insufficient User Role	Login failed due to insufficient user role.
RT_INVALID_PASSWORD	Invalid Password	Login failed due to invalid username/password.
RT_NOT_ENOUGH_RPC_ HANDLES	Not Enough RPC Handles	Login failed due to insufficient number of RPC handles (20 max).

Access control

An SMI client uses a two-level login: one login to the SMI-A and another login to the proxy switch to gain access to a fabric. The SMI-A has a limitation of one connection per fabric, so all SMI clients share the same connection to a fabric even if they have different Role-Based Access Control (RBAC) roles.

To enable SMI clients to have different RBAC roles, you can map each SMI client to a different switch user. With this mapping, SMI clients can have different RBAC roles, even though they share the same connection to the fabric.

For additional information about RBAC roles, see the *Brocade SMI Agent Developer's Guide*.

The Brocade SMI Agent Configuration Tool has two Access Control options:

- User Mapping
- Default User Mapping

The User Mapping option allows you to map specific SMI-A users to specific switch user names. The Default User Mapping option allows you to set up the mapping for all other SMI-A users. Using these two options, you can restrict access to specific SMI-A users. For example, in the User Mapping section you can specify a few SMI-A users who have admin-level access and give all the other SMI-A users user-level access in the Default User Mapping section.

Mapping an SMI-A user to a switch user

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **User Mapping** in the menu tree (see Figure 6 on page 19).

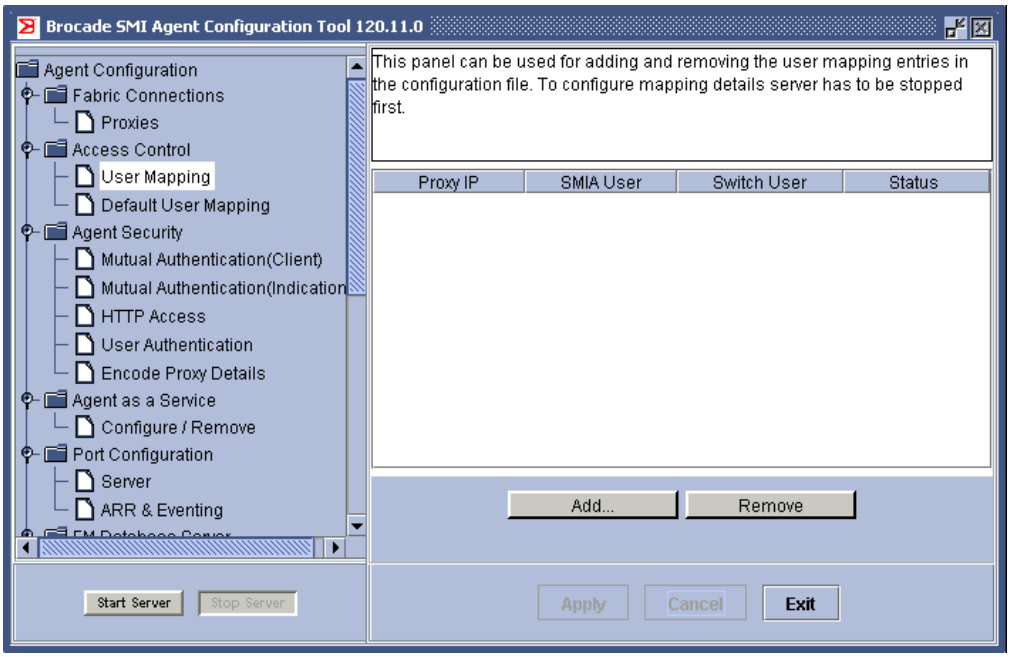


FIGURE 6 User mapping

3. Click the **Stop Server** to stop the SMI-A, if it is running. This button is unavailable if the server is already stopped.
4. Click **Add**.
5. Fill out the **User Mapping Configuration** dialog box and click **OK**.

   The **Proxy IP**, **SMIA User name**, and **Switch User name** fields are mandatory. The **Password** field is mandatory if Radius Server Authentication is enabled; otherwise, it is optional. If you enter a password, it must be valid, even if it is optional.

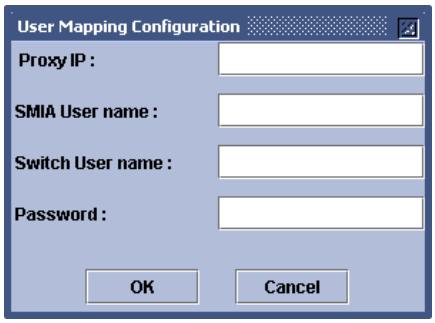


FIGURE 7 User Mapping Configuration dialog box

6. Repeat step 4 through step 5 to map additional user names.
7. Click **Apply**.

The value in the **Status** column changes from **Not Persisted** to **Persisted**, which means the values are persisted to the *provider.xml* configuration file.

Setting up default SMI-A user mapping

You can set up a default mapping that applies to all SMI-A users that are not explicitly mapped in the User Mapping section.

If a default mapping is not provided, then all unmapped SMI-A users inherit the same access as the account used to connect to the switch.

Only one default mapping scheme is allowed for each fabric.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Default User Mapping** in the menu tree (see Figure 8).

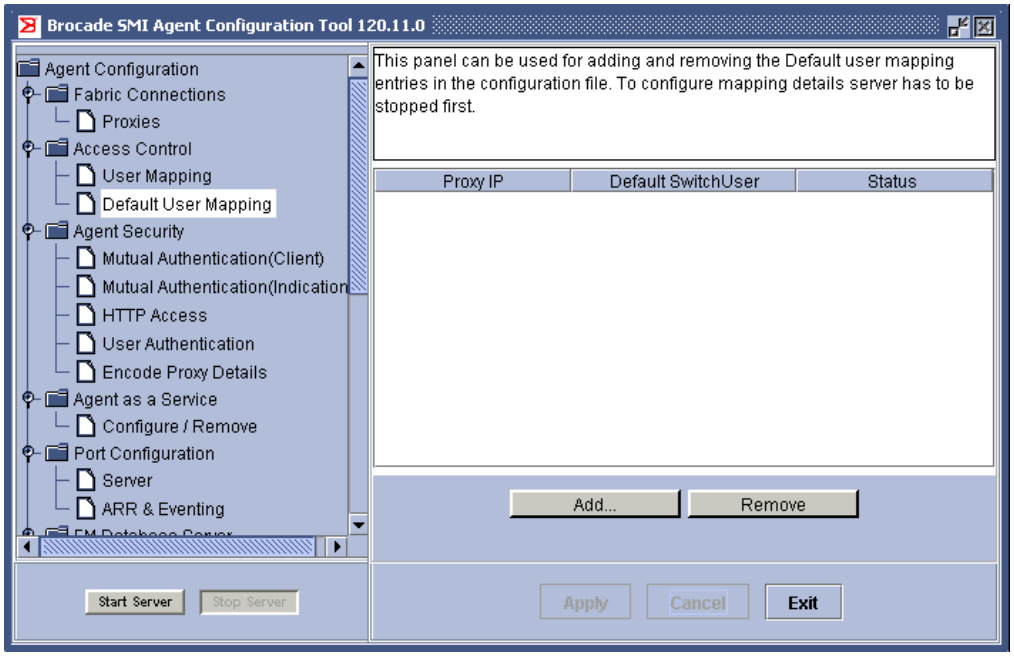


FIGURE 8 **Default user mapping**

3. Click the **Stop Server** to stop the SMI-A, if it is running. This button is unavailable if the server is already stopped.
4. Click **Add**.
5. Fill out the **Default User Mapping Configuration** dialog box and click **OK**.

   The **Proxy IP** field is optional. If you do not specify the IP address of the proxy switch, then all unmapped SMI-A users can access the fabric with the same RBAC role as the given switch user name.

   The **SMIA SwitchUser** field is mandatory.

   The **Default User Password** field is mandatory if Radius Server Authentication is enabled; otherwise, it is optional. If you enter a password, it must be valid, even if it is optional.

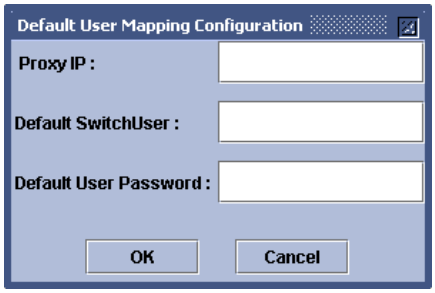


FIGURE 9 User Mapping Configuration dialog box

6. Click **Apply**.

   The value in the **Status** column changes from **Not Persisted** to **Persisted**.

Limitations of SMI-A user-to-switch user mapping

- Indications are not filtered based on the SMI-A user names. Indications related to fabrics for which the SMI-A user does not have access will still be delivered.
- It is not recommended to map default SMI-A users to a zoneadmin switch user. If default SMI-A users are mapped to a zoneadmin switch user, then the Brocade SMI Agent Configuration Tool is unable to display the status of the fabric connection.
- For VF-enabled chassis, read or write access restrictions are not allowed for each logical fabric separately. If the SMI-A user is mapped to a switch user on a VF-enabled chassis, then the SMI-A user has the same access privilege for all of the logical fabrics in the chassis.
- For VF-enabled chassis, the switch user mapped in User mapping and Default User mapping configurations should have access to at least one of the logical fabrics configured in the VF-enabled chassis.
- The SMI Agent does not restrict access based on the VF list accessible to the switch user in a VF-enabled chassis. The SMI Agent uses the RBAC permission map of the proxy switch alone. For switches running Fabric OS 6.3.x or earlier, RBAC restrictions in the SMI Agent cannot be specific to certain logical fabrics. To get the same RBAC behavior in the SMI Agent for switches running Fabric OS 6.4.x or later, the chassis role of these switches should not be more access restrictive than the switch role.

SMI Agent security

This section describes how to use the Brocade SMI Agent Configuration Tool to configure security options.

Mutual authentication setup

Before you enable mutual authentication for clients and indications, you need to do the following so the Configuration Tool will know the location of the certificate files:

- Configure the *WbemClient.properties* file with the location of the certificate files.
- Update the CLASSPATH variable in two files with the location of the *WbemClient.properties* file.

Configuring mutual authentication for clients

You can restrict access to the SMI-A to only clients that are trusted by the agent. The SMI-A uses private key information and authentication information to allow only specific clients to send requests as SSL-encrypted CIM-XML to the SMI-A.

By default, mutual authentication for clients is disabled, which means that any client can use the HTTPS communication protocol to communicate with the SMI-A. When mutual authentication for clients is enabled, then only those clients whose certificates have been added to the SMI-A TrustStore can use HTTPS to communicate with the SMI-A. That is, the SMI-A must have a TrustStore that contains a certificate for an entry in the client KeyStore.

Additionally, when mutual authentication for clients is enabled, the client must have a TrustStore that contains the certificate for an entry in the SMI-A KeyStore.

Using the Brocade SMI Agent Configuration Tool, you can enable and disable mutual authentication for clients, import the client certificate to the SMI-A TrustStore, and export the server certificate to a file where the client can access it.

If you enable mutual authentication, you may choose to disable the CIM-XML client protocol adapter (CPA) for the SMI-A so that the clients can use only HTTPS communication. If you do not disable the CIM-XML CPA, then any client can communicate with the SMI-A using HTTP access.

When you disable or enable mutual authentication for clients, the SMI-A server must be stopped.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Mutual Authentication(Client)** in the menu tree (see Figure 3 on page 14).

   The content pane displays the current setting, which is selected and dimmed.
3. To enable mutual authentication for clients, click the **Enable Client Authentication** radio button. If this option is unavailable, then mutual authentication for clients is already enabled.

   To disable mutual authentication for clients, click the **Disable Client Authentication** radio button. If this option is unavailable, then mutual authentication for clients is already disabled.
4. Click the **Stop Server** to stop the SMI-A, if it is running. This button is unavailable if the server is already stopped.
5. Click **Apply**.
6. If you *enabled* mutual authentication for clients, you can perform the following optional steps to allow only secure communication with trusted clients:

   a. Disable HTTP access so that only HTTPS access is available to the clients. (See "Configuring HTTP access" on page 24.) Clients should preferably use HTTPS for all communications purposes if mutual authentication is enabled.

      If you do not disable HTTP access, then any client can communicate with the SMI-A using HTTP access.

b. Configure the WBEM client to use client certificates to communicate with the SMI-A. (See "Client configuration to use client certificates" on page 48.)

The changes take effect when you restart the server. Click **Start Server** to restart the server.

Configuring mutual authentication for indications

By default, mutual authentication for indications is disabled, which means that the SMI-A uses SSL to send CIM-XML indications to a WBEM client listener, but does not attempt to verify the identity of the WBEM client listener. When mutual authentication for indications is enabled, then only those clients whose certificates have been added to the SMI-A Indications TrustStore can use SSL to receive indications from the SMI-A. That is, the SMI-A must have a TrustStore that contains a certificate for an entry in the client's Indications KeyStore.

When you disable or enable mutual authentication for indications, the SMI-A server must be stopped.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Mutual Authentication(Indication)** in the menu tree (see Figure 10 on page 24).

   The content pane displays the current setting, which is selected and dimmed.
3. To enable mutual authentication for indications, click the **Enable Indication Authentication** radio button. If this option is unavailable, then mutual authentication for indications is already enabled.

   To disable mutual authentication for indications, click the **Disable Indication Authentication** radio button. If this option is unavailable, then mutual authentication for indications is already disabled.
4. Click the **Stop Server** to stop the SMI-A, if it is running. This button is unavailable if the server is already stopped.
5. Click **Apply**.
6. If you enabled mutual authentication for indications, you can perform the following optional steps to allow only secure communication with trusted clients:

   a. Disable HTTP access so that only HTTPS access is available to the clients. (See "Configuring HTTP access" on page 24.) Clients should preferably use HTTPS for all communications purposes if mutual authentication is enabled.

      If you do not disable HTTP access, then any client can communicate with the SMI-A using HTTP access.

   b. Configure the WBEM client to use client certificates to communicate with the SMI-A. (See "Client configuration to use client certificates" on page 48.)

The changes take effect when you restart the server. Click **Start Server** to restart the server.

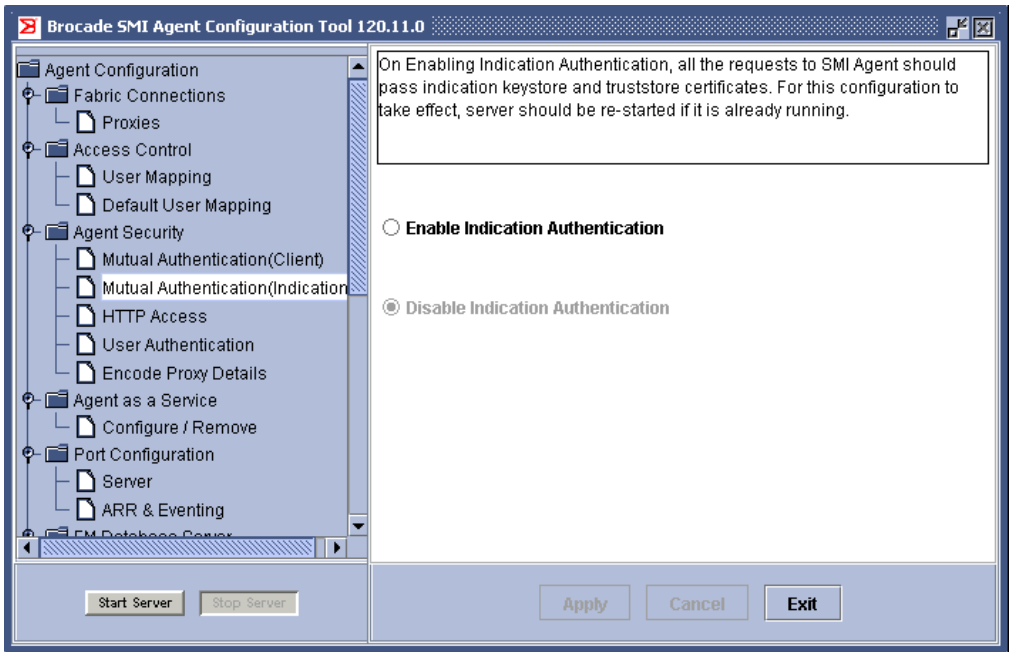


FIGURE 10 **Mutual authentication for indications**

Configuring HTTP access

When HTTP access is disabled, only HTTPS access is available to the clients. The SMI-A server must be stopped to enable HTTP access, and must be running to disable HTTP access.

You must have Administrator privileges (Windows) or root/admin privileges (Linux, Solaris, and AIX) to enable or disable HTTP access. This option is disabled if you do not have the appropriate privilege.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **HTTP Access** in the menu tree (see Figure 11).

   The content pane displays the current setting, which is selected and unavailable. If the SMI-A server is not running, the Configuration Tool cannot determine whether HTTP access is enabled and so displays the default setting and not the current setting.
3. To change the HTTP access setting, click the button of the available option.

   If HTTP access is already enabled, the **Disable HTTP Access** option is available.
   If HTTP access is already disabled, the **Enable HTTP Access** option is available.
4. Perform one of the following actions:

   To enable HTTP access, ensure that the SMI-A server is stopped. Click the **Stop Server** button.
   To disable HTTP access, ensure that the SMI-A server is running. Click the **Start Server** button.
5. Click **Apply**.

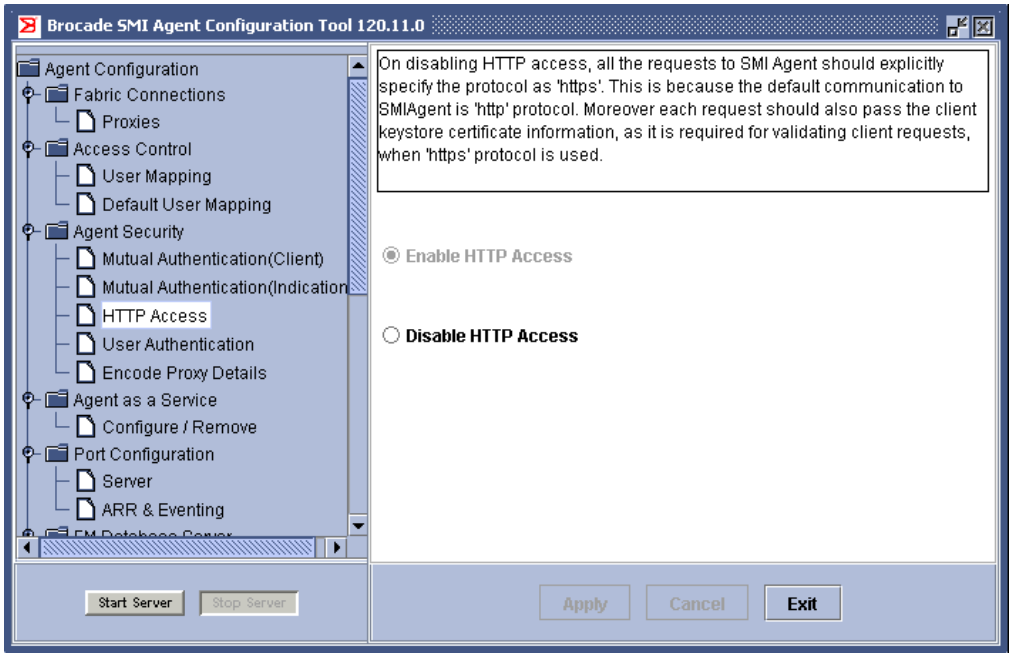


FIGURE 11 HTTP access

Importing client certificates

If you enable mutual authentication for clients or mutual authentication for indications, you can import a client certificate into the SMI Agent server truststore. This certificate will be used for authentication if mutual authentication is enabled.

NOTE
You can import only certificates generated using Java Keytool or OpenSSL.

If mutual authentication is enabled and if you do not provide a security certificate, then the Brocade-provided client certificate (`client.cer`) will be used to authenticate clients.

You must have Administrator privileges (Windows) or root/admin privileges (Linux, Solaris, and AIX) to import client certificates. This option is disabled if you do not have the appropriate privilege.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Import** in the menu tree (see Figure 12).

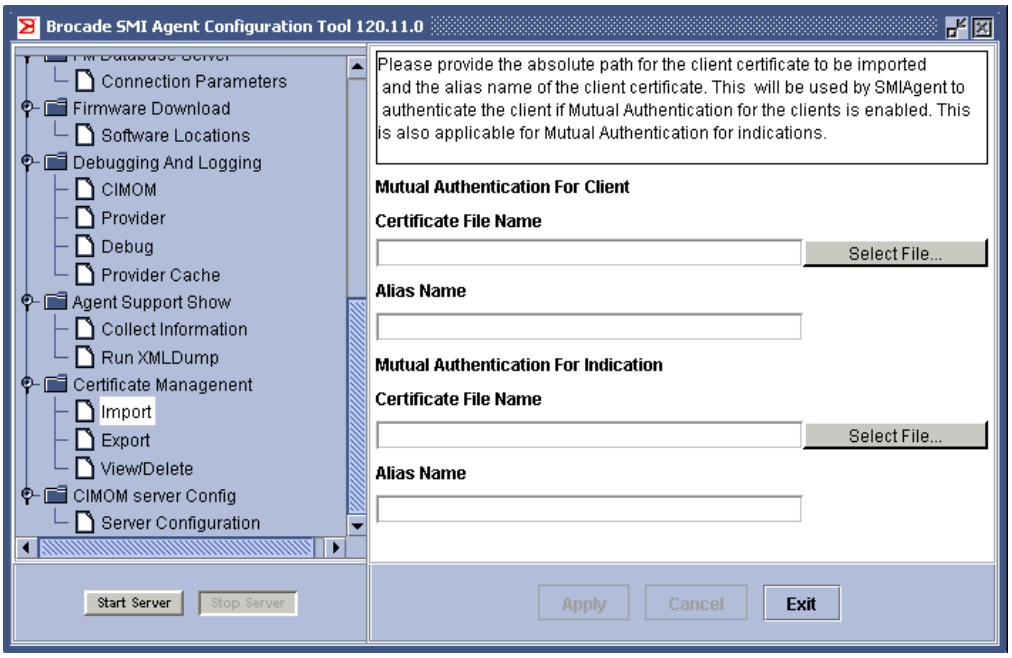


FIGURE 12 Importing client certificates

3. Enter information for the client certificate to be used for mutual authentication for clients.
    a. Type the path of the client certificate in the **Certificate File Name** field, or click **Select File** to browse for the file.
    b. Type the alias name of the certificate in the **Alias Name** field.
4. Enter information for the client certificate to be used for mutual authentication for indications.
5. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

Exporting server certificates

If you enable mutual authentication for clients or mutual authentication for indications, you can export the corresponding SMI-A server certificate to a file so the client can add the certificate to its TrustStore. This certificate will be used for authentication if mutual authentication is enabled.

If mutual authentication is enabled and if you do not export the SMI Agent server certificate, then the client keystore, truststore, and server certificates will be used for authentication.

You must have Administrator privileges (Windows) or root/admin privileges (Linux, Solaris, and AIX) to export server certificates. This option is disabled if you do not have the appropriate privilege.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Export** in the menu tree (see Figure 13).

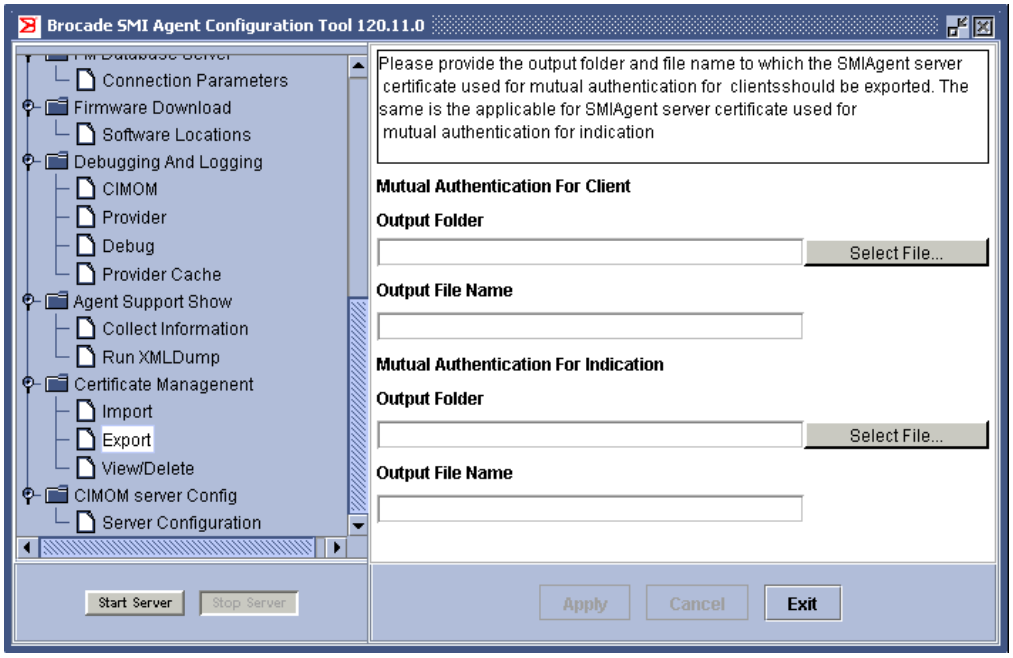


FIGURE 13 **Exporting client certificates**

3. Enter the output folder and file name for the certificate used for mutual authentication for clients.
    a. Type the path of the output folder to which the server certificate will be exported in the **Output Folder** field, or click **Select File** to browse for the file.
    b. Type the file name in the **Output File Name** field.
4. Enter the output folder and file name for the certificate used for mutual authentication for indications.
5. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

Viewing or deleting client certificates from SMI-A server truststore

You can use the Brocade SMI Agent Configuration Tool to view and delete client certificates that have been added to the SMI-A server truststore.

You must have Administrator privileges (Windows) or root/admin privileges (Linux, Solaris, and AIX) to view or delete client certificates. This option is disabled if you do not have the appropriate privilege.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **View/Delete** in the menu tree (see Figure 14).

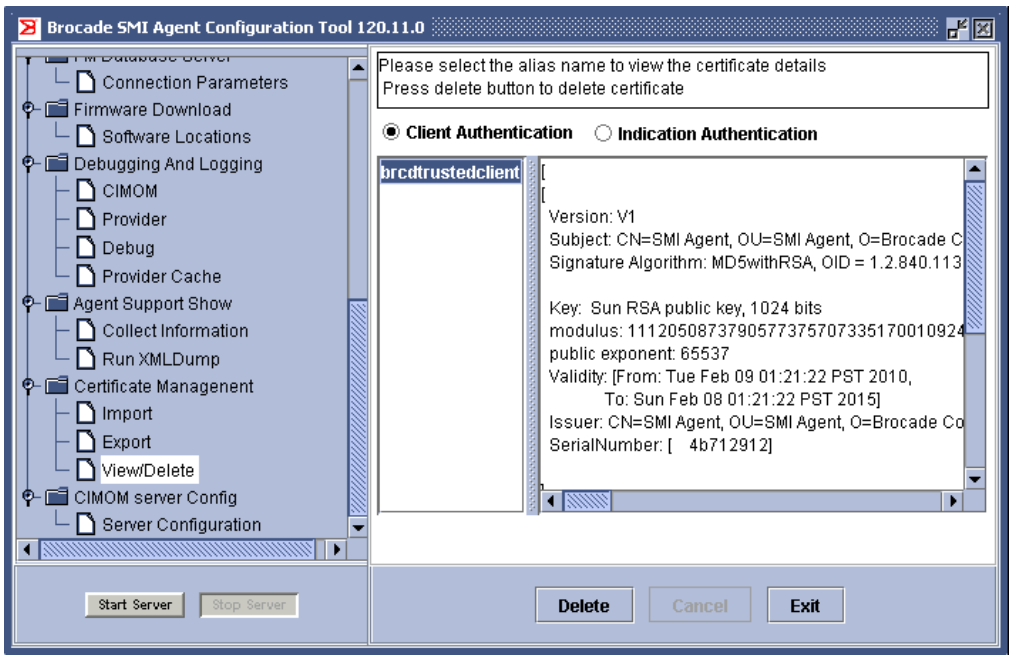


FIGURE 14 **Viewing and deleting client certificates in server truststore**

3. Click **Client Authentication** or **Indication Authentication** to view the corresponding list of certificates.
4. Select the certificate in the left side of the pane.

   The right side of the pane displays the selected certificate. Use the scroll bars to view the certificate.
5. To delete the selected certificate from the SMI-A truststore, click **Delete**, and click **Yes** in the confirmation window.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

Configuring user authentication

You must have Administrator privileges (Windows) or root/admin privileges (Unix) to configure user authentication. This option is disabled if you do not have the appropriate privilege.

The SMI-A server should be running while enabling or disabling Windows Domain Authentication. Enabling and disabling Windows Domain Authentication is applicable only for the Windows platform.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **User Authentication** in the menu tree (see Figure 15 on page 29).

   The content pane displays the current setting, which is selected and dimmed.
3. To change the user authentication setting, click the button of the available option.

   If user authentication is already enabled, the **Disable User Authentication** option is available. If user authentication is already disabled, the **Enable User Authentication** option is available.

Disabling user authentication does not take effect until after the server is restarted. So even if you disable user authentication in this window, you will still be prompted to provide user credentials until you restart the server.

4. *Windows only:* You can enable domain authentication by checking the **Windows Domain Authentication** check box and providing the domain name in the field provided.

   To disable domain authentication, clear the **Windows Domain Authentication** check box. If you disable the Windows domain authentication, you are prompted to provide local user credentials.

   This option is available only if you clicked **Enable User Authentication** or if user authentication is already enabled.

5. Click **Apply**.

   If you enabled user authentication, a dialog box pops up requesting user name and password.

6. Provide the user name and password in the dialog box. Do not include the domain name with the user name. For example:

   Correct user: myUserName

   Incorrect user: myDomain\myUserName

   These credentials are assumed to be valid and are not authenticated by the Configuration Tool. These credentials are used in further communication with the SMI Agent.

   If Windows Domain Authentication is not enabled, then provide the local user credentials. If Windows Domain Authentication is enabled, then provide the domain user credentials.

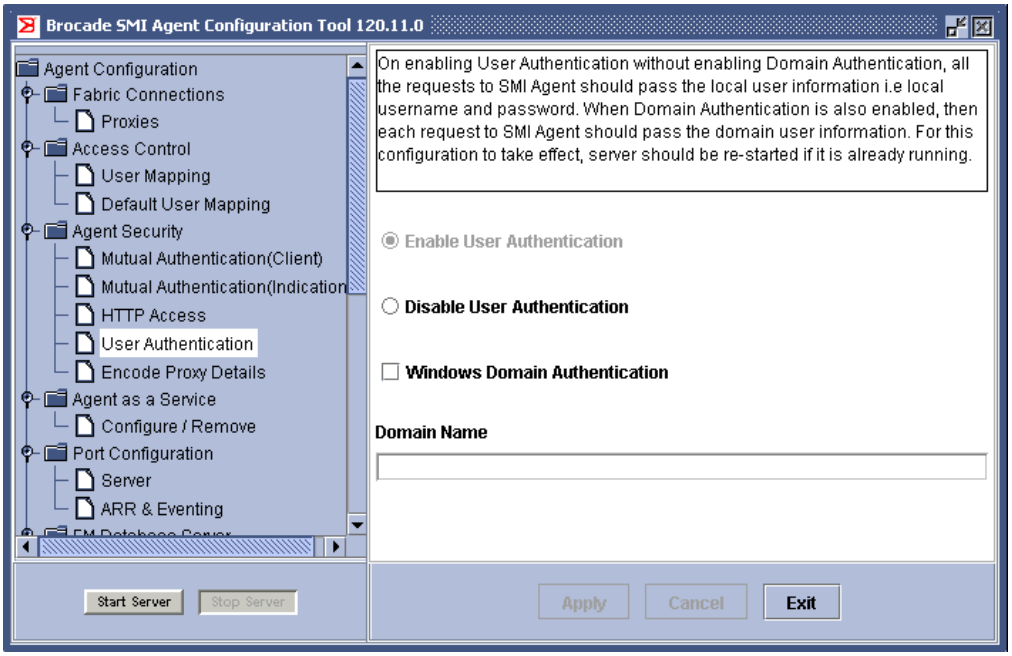


FIGURE 15 **User authentication**

Encoding proxy connection details

For additional security you can encode the contents of the *provider.xml* file.

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Encode Proxy Details** in the menu tree (see Figure 16).

   The content pane displays the current setting, which is selected and dimmed.
3. Click the **Stop Server** to stop the SMI-A, if it is running. This button is unavailable if the server is already stopped.
4. To change the encoding setting, click the button of the available option.

   If encoding is already enabled, the **Disable Proxy Connection Details Encoding** option is available.

   If user authentication is already disabled, the **Enable Proxy Connection Details Encoding** option is available.
5. Click **Apply**.

   If you enabled encoding, the proxy connection entries are removed from the *provider.xml* file are copied to the *provider.ser* binary file. New proxy entries are also written to the *provider.ser* file.

   If you disabled encoding, the proxy connection entries are removed from the *provider.ser* binary file and copied to the *provider.xml* file. New proxy entries are also written to the *provider.xml* file.

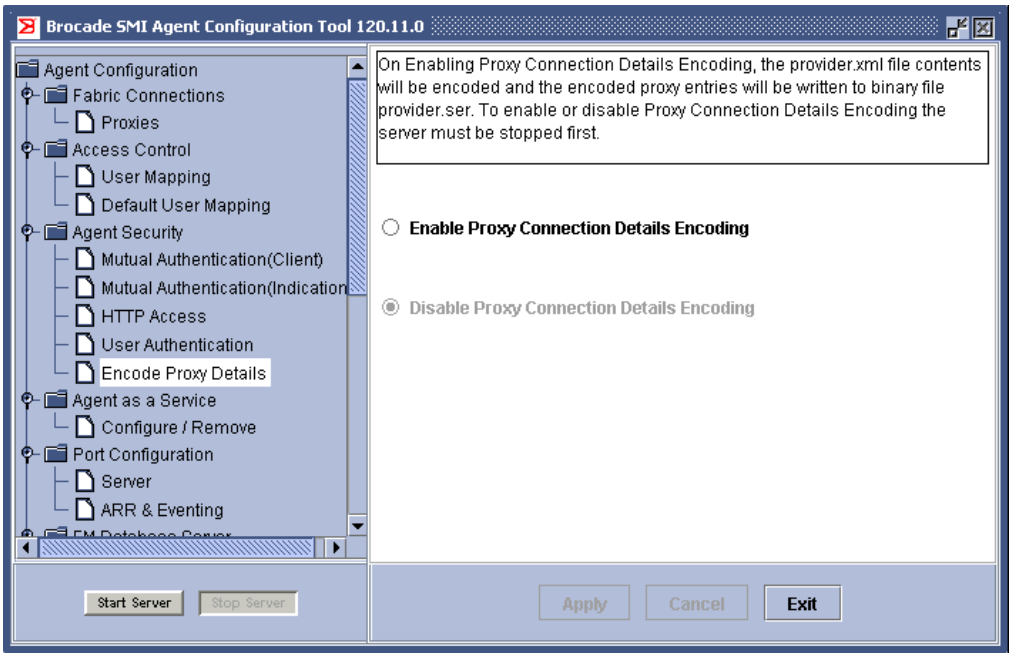


FIGURE 16 Encode proxy details

SMI Agent service configuration and removal

You must have Administrator privileges (Windows) or root/admin privileges (Linux, Solaris, and AIX) to configure or remove the SMI Agent as a service. This option is disabled if you do not have the appropriate privilege.

Configuring or removing the SMI Agent as a service

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Configure / Remove** in the menu tree (see Figure 17).

   The content pane displays the current setting, which is selected and dimmed.
3. To change the setting, click the button of the available option.

   If the SMI Agent is installed as a service, the **Remove as a Service** option is available.
   If the SMI Agent is not installed as a service, the **Configure as a Service** option is available.
4. Click **Apply**.

   If you selected to configure the SMI Agent as a service, the SMI Agent is installed and started as a service. The name of the service is “Brocade SMI Agent (J WBEM Server)”.

   If you selected to remove the SMI Agent as a service, the SMI Agent is stopped (if it is running as a service) and uninstalled.

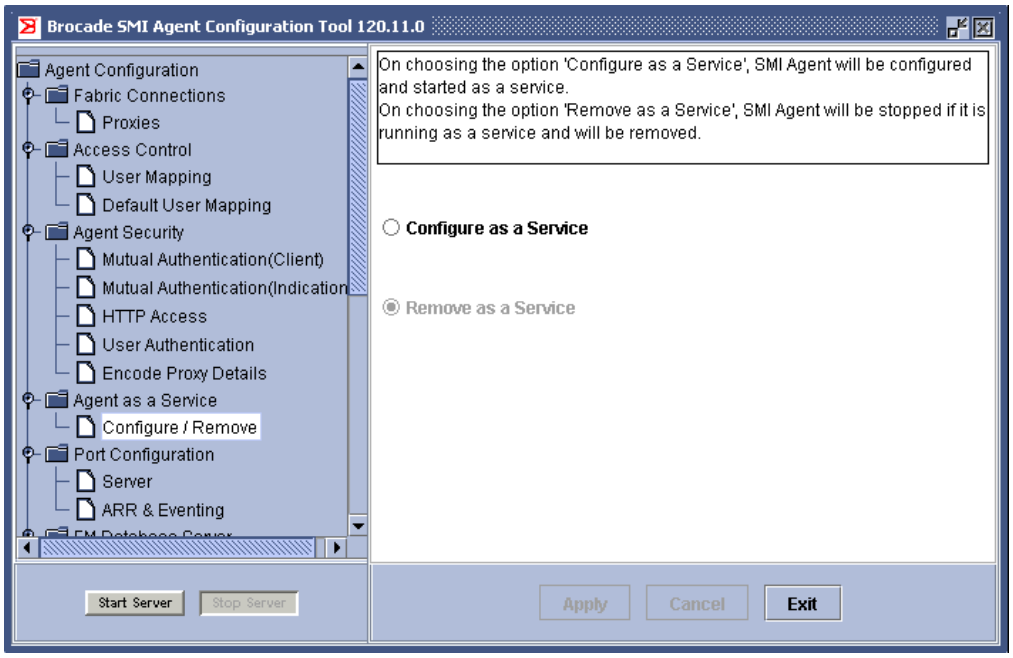


FIGURE 17 **Configure or remove SMI Agent as a service**

Port configuration

This section describes how to configure the HTTP, HTTPS, ARR, and Eventing ports.

Configure HTTP and HTTPS ports

The SMI-A includes the CIM-XML and CIM-XMLS Client Protocol Adapters (CPA). By default, all are installed and enabled for use. Each CPA uses a different TCP port to exchange WBEM requests and responses. By default, the SMI-A has configured its supported CPAs to use the following ports:

- CIM-XMLS (HTTPS) on TCP port 5989
- CIM-XML (HTTP) on TCP port 5988

If multiple CIM agents are running at the same time on a system, they cannot use the same ports. For example, some operating systems (such as Solaris 8 and Solaris 9) have a CIM agent preinstalled and already running on standard CIM TCP ports. This can cause conflicts with the SMI-A if both agents are listening on the same ports. In this case, you must configure each SMI-A to use different ports. Refer to your operating system documentation for more information on whether a CIM agent is running.

When you choose values for the HTTP and HTTPS ports, make sure they are not one of the assigned TCP ports. The Configuration Tool does not check for this. You can see a list of assigned TCP ports at:

http://www.iana.org/assignments/port-numbers

Configuring the HTTP and HTTPS ports

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Server** in the menu tree (see Figure 18 on page 33).

   The content pane displays the current and configured HTTP and HTTPS ports.

   Current means the SMI Agent is currently using these ports, provided the server is running. *Configured* means the configuration is not in effect currently, but will be used when the server is restarted.
3. To change the settings, type new values in the **Configured HTTP Port** and **Configured HTTPS Port** fields.

   The value must be between 1 and 65535, inclusive.

   Make sure the ports are not in use before you assign them; otherwise, the results will be unpredictable.
4. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

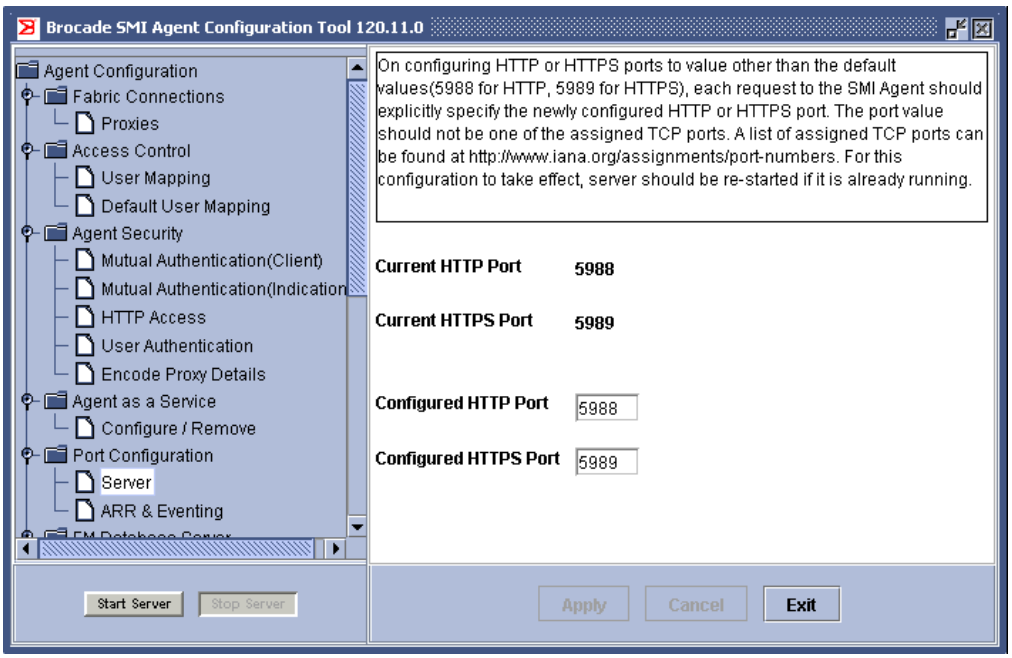


FIGURE 18 Configure HTTP and HTTPS ports

Configure ARR and eventing ports

You can configure both the secure and non-secure ARR and eventing ports using the procedure in this section.

The *ARR port* is the port through which the switches in the fabric send data (large payload responses) back to the SMI-A.

The *eventing port* is the port through which the switch connects to the SMI-A to deliver events.

If a firewall exists between the SMI-A and the fabric, these ports must be open in the firewall. If these ports are not open, the connection from the SMI-A to the fabric will fail.

ARR and eventing ports are optional. If you do not configure them, or if you configure them with a value of 0, the SMI Agent dynamically allocates a port during server startup.

When you choose values for the ARR and eventing ports, make sure they are not one of the assigned TCP ports. The Configuration Tool does not check for this. You can see a list of assigned TCP ports at:

http://www.iana.org/assignments/port-numbers

Configuring the ARR and eventing ports

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **ARR & Eventing** in the menu tree (see Figure 19 on page 34).

   The content pane displays the current ARR and eventing ports.
3. To change the settings, type new values in the fields.

   The value must be between 0 and 65535, inclusive. If the value is 0, the SMI Agent dynamically allocates a port during server startup.

4. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

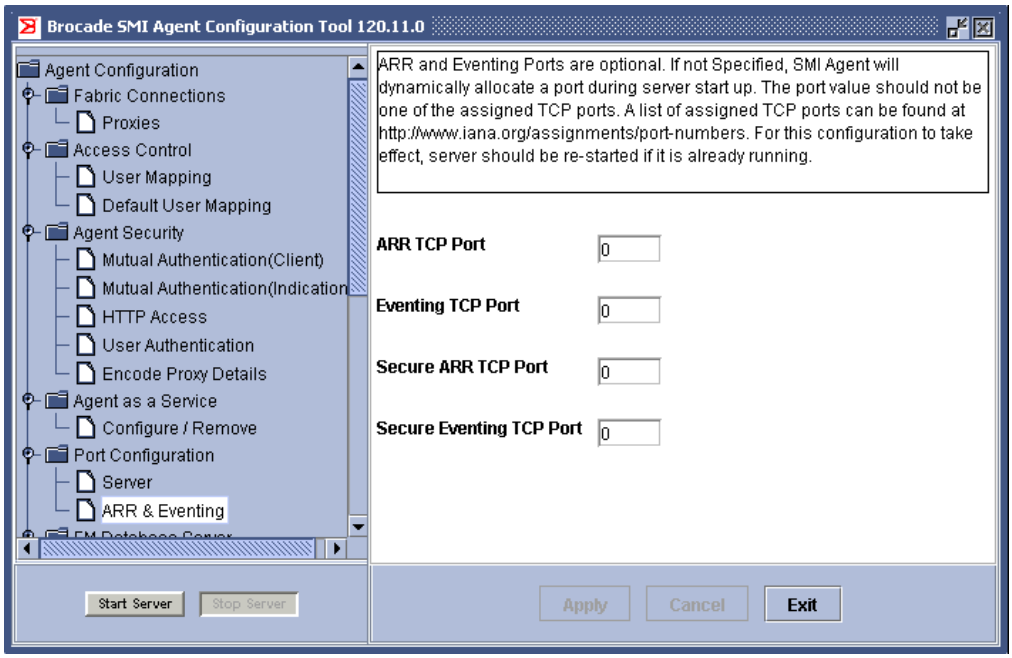


FIGURE 19 **Configure ARR and eventing ports**

Fabric Manager database server configuration

Configuring a Fabric Manager database server connection allows the Brocade SMI Agent to report on historical port statistics by retrieving the data from the Fabric Manager database server. Not all users have a Fabric Manager server installed and running in their environment. Here you can specify the connection information for an existing Brocade Fabric Manager server. If your management application does not make use of historical port statistics, you do not need to configure a connection to the Fabric Manager database.

The Fabric Manager Database server TCP/IP listener is always started on port 2638, which is registered with Internet Assigned Numbers Authority (IANA). Database connection credentials are not user-customizable and are fixed at the factory.

Configuring the Fabric Manager database server connection parameters

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Connection Parameters** in the menu tree (see Figure 20).

   The content pane displays the current connection parameters.

   The **Driver** field is already populated with the default driver that is bundled in the agent: **com.sybase.jdbc2.jdbc.SybDriver**.

   Do not change this driver information.

3. To change the settings, type new values in the **URL**, **User Name**, and **Password** fields:

   URL URL to locate the database. If the Fabric Manager server is installed on the same host as the SMI-A, the URL is:
   jdbc:sybase:Tds:localhost:2638/fabman
   Otherwise, replace **localhost** with the Fabric Manager server's host IP address, in IPv4 or IPv6 format.

   User Name User name for the database user. Default DSN user name is: **dba**

   Password Password for the database user. Default DSN password is: **sql**

4. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

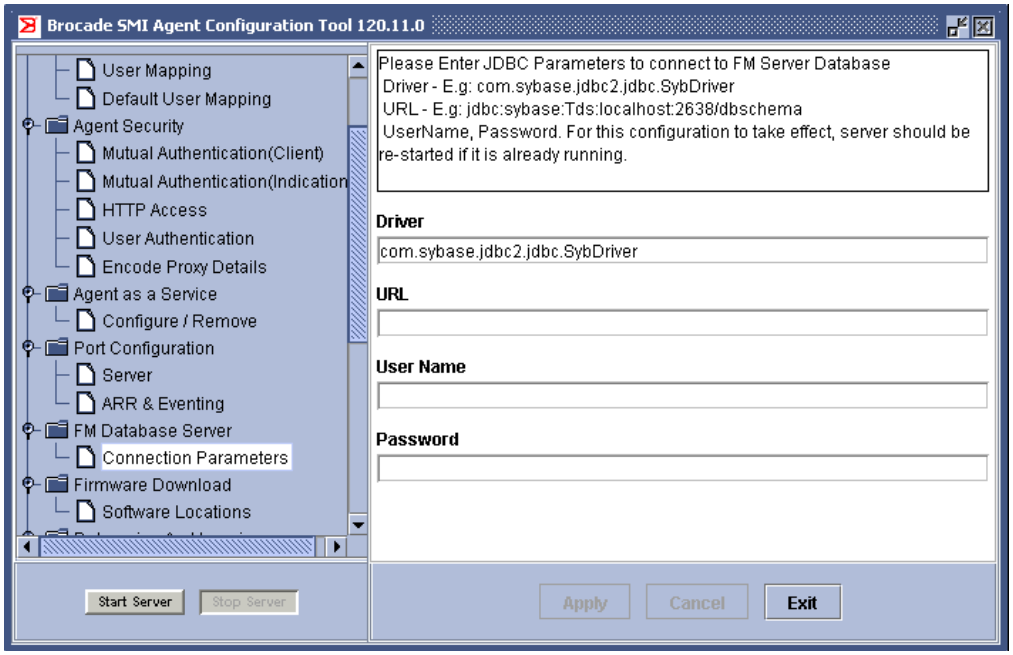


FIGURE 20 **Configure Fabric Manager database server connection parameters**

Firmware download software locations configuration

Use the following procedure to add, modify, or remove software locations for firmware download.

Configuring software locations for firmware download

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Software Locations** in the menu tree (see Figure 21 on page 36).

   The content pane displays the current software locations.

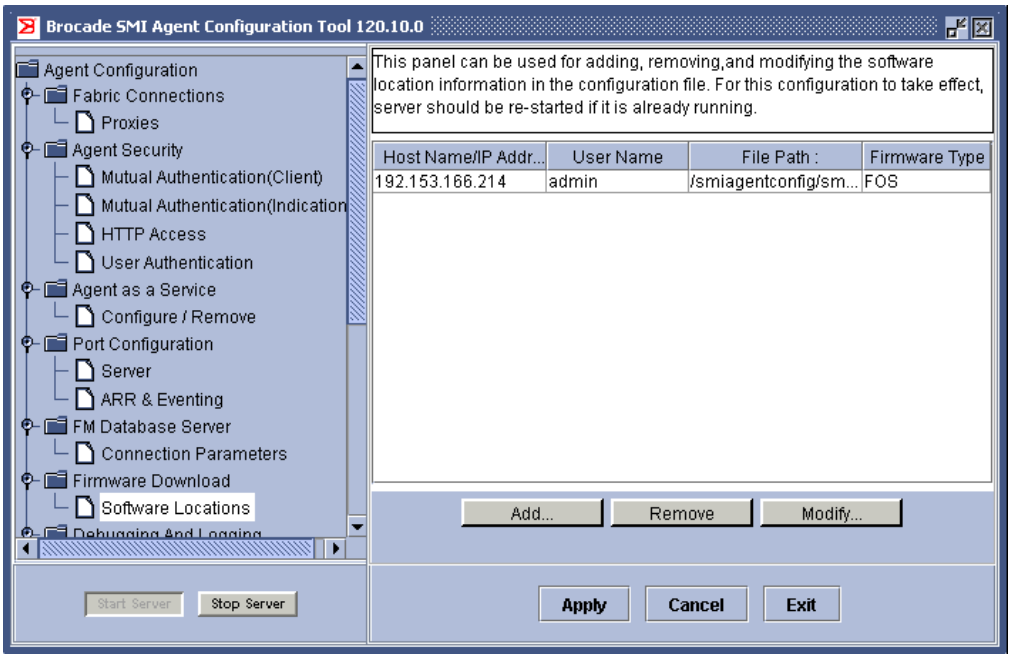


FIGURE 21 **Configure firmware download software locations**

3. To add a new entry, click the **Add** button and fill out the **Software Location** dialog box (Figure 22) with the following values:

   HostName/IP Address Type the host name or host IP address (in IPv4 or IPv6 format).

   User name and **Password** Type the user name and password with which to log in to the host.

   File Path Type either the absolute or relative path to the software file.

   Firmware Type Select either FOS or SAS from the drop-down list.

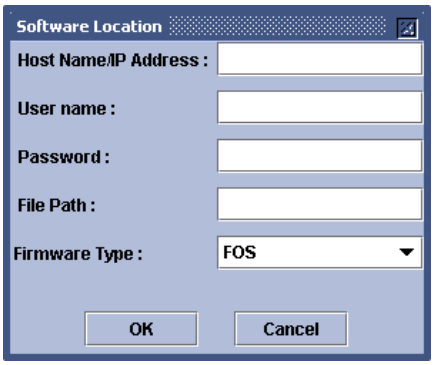


FIGURE 22 **Software Location dialog box**

   To modify an existing entry, select the entry in the content pane, click the **Modify** button, and fill out the **Software Location** dialog box. You can modify only one entry at a time.

   To remove an existing entry, select the entry in the content pane and click the **Remove** button.

4. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

Debugging and logging options configuration

This section explains how to use the Brocade SMI Agent Configuration Tool to configure debugging and logging options for the CIMOM and Provider. This information can be useful in diagnosing problems during development of client applications, providers, and other components.

Debugging options for CIMOM

The SMI-A can write detailed debugging output to a file. By default, the SMI-A is configured with debugging disabled.

You can enable or disable debugging for CIMOM using the Brocade SMI Agent Configuration Tool. If you enable debugging, trace statements are logged to a trace file with the following name format:

jserverlog_<month & date>_<Hour & Mins>.trace

For example, *jserverlog_1017_1655.trace* is the trace file for 4:55 p.m. on October 17.

Whenever the CIMOM server is restarted, a new trace file is generated with the timestamp of when the server starts.

The location of this log file is the folder from which the SMIA server is started. It is usually the folder that contains the start_server script:

On Linux, Solaris, and AIX:*<SMIAgent>/agent/server/jserver/bin*

On Windows: *<SMIAgent>\agent\server\jserver\bin*

Configuring debugging options for CIMOM

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **CIMOM** in the menu tree (see Figure 23 on page 38).

   The content pane displays the current debugging configuration for CIMOM. By default, debugging is disabled (log level = NO LOG).
3. Select a log level value from the list. Possible values are:

• NO LOG	10000	Do not log (default).
• SEVERE	1000	Log severe error messages.
• WARNING	900	Log warning messages.
• INFO	800	Log informational messages.
• CONFIG	700	
• FINE WITH XML TRACE	500	Log detailed trace information, including Server XML Trace output.
• FINER	400	
• FINEST	300	
• ALL	0	Log all messages.

   Selecting NO LOG disables logging. Selecting any value other than NO LOG enables logging.

4. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

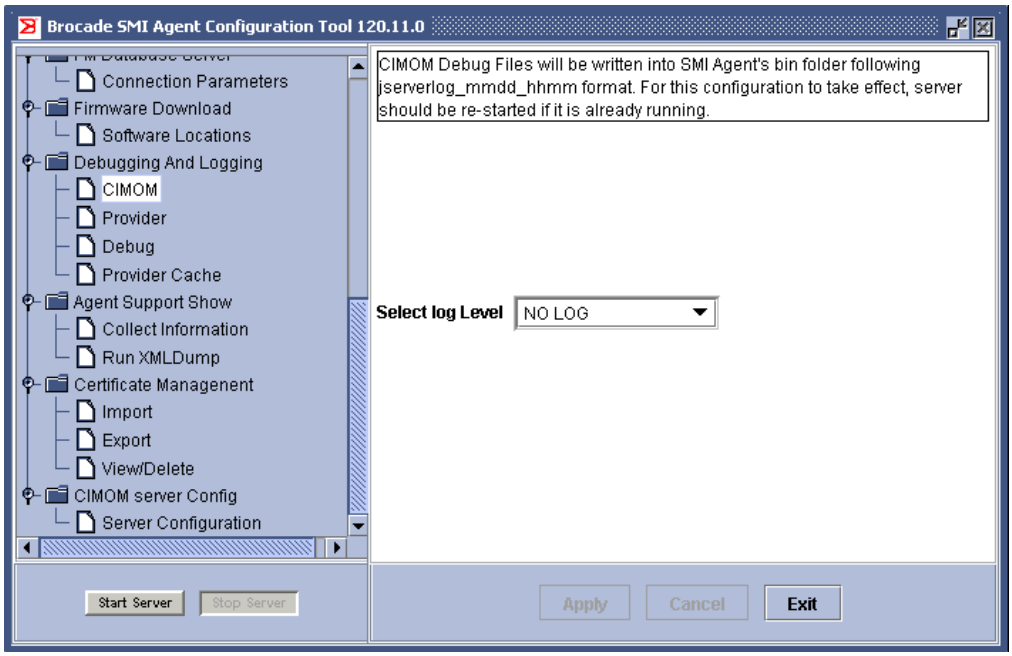


FIGURE 23 Configure debugging options for CIMOM

Debugging options for the provider

This section describes how you can update the debugging configuration. By default, debug logging for the provider is enabled.

You can update debugging configuration dynamically or you can update the debug properties file. If you update dynamically, your changes are effective immediately, but are not saved. If you update the debug properties file, your changes are saved, but are not reflected until the server is restarted.

You can specify a file to be the debug properties file, or you can use the default file, which is in the following location:

On Linux, Solaris, and AIX:*<SMIAgent>/agent/server/jserver/bin/debug.properties*

On Windows: *<SMIAgent>\agent\server\jserver\bin\debug.properties*

You can set the following debug options:

- Exception
- Operation
- Event
- Configuration
- Switch Data
- Switch XML Data
- Threadlock

Switch Data and Switch XML Data are used internally for communication with the switch.

Configuring debugging options for the provider

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Debug** in the menu tree (see Figure 24 on page 40).

   The content pane displays the current debugging configuration for the provider.
3. To enable debugging:
   a. Check the **Enable Debug logging** check box.
   b. Click one of the following:
      - **Dynamic Update**

        Update the configuration immediately, when you click **Apply**. The configuration changes are not saved when the server is stopped.
      - **File Update**

        Save the changes to the configuration file when you click **Apply**. The configuration changes are not reflected until you restart the server. The changes are written to the configuration file shown in the **Debug Configuration file** field; you can click **Select File** to select a different file.
   c. If you checked the **Enable Debugging** option, check the debug options you want to log. You can set the following debug options:
      - Exception
      - Operation
      - Event
      - Configuration
      - Switch Data
      - Switch XML Data
      - Threadlock
   d. If you checked the **Exception debug** option, select the exception level from the drop-down list.

      You set an exception level to suppress logging unwanted exceptions. Setting an exception level causes the SMI-A to log all exceptions of that level and lower. For example, setting an exception level of 3 logs exceptions having values of 1, 2, and 3, but does not log level 4 exceptions.

      The exception level values are:

0	No exceptions are logged.
1 - Fatal	Exceptions that affect further functioning of the SMI-A. For example, exceptions when rpcd fails on the switch.
2 - Error	Exceptions that are important and directly affect client operation. For example, an exception when the call for getting Brocade_SwitchFCPort information fails.
3 - Warning	Exceptions that need user attention, but do not directly affect SMI-A functionality. For example, an exception logged when the password is expiring on the proxy switch.

4 - Info	Exceptions that are of no interest to the user. For example, an exception logged when the SMI-A first attempts a secure login to a non-secure switch if the user specifies “ProtocolToUse” as “Any.”

NOTE
Increasing the value of the exception level causes a decrease in performance because the amount of data to be logged increases.

4. To disable debugging, clear the **Enable Debug logging** check box.
5. Click **Apply**.

If you selected **Dynamic Update**, the changes take effect immediately. If you selected **File Update**, the changes take effect when you restart the server.

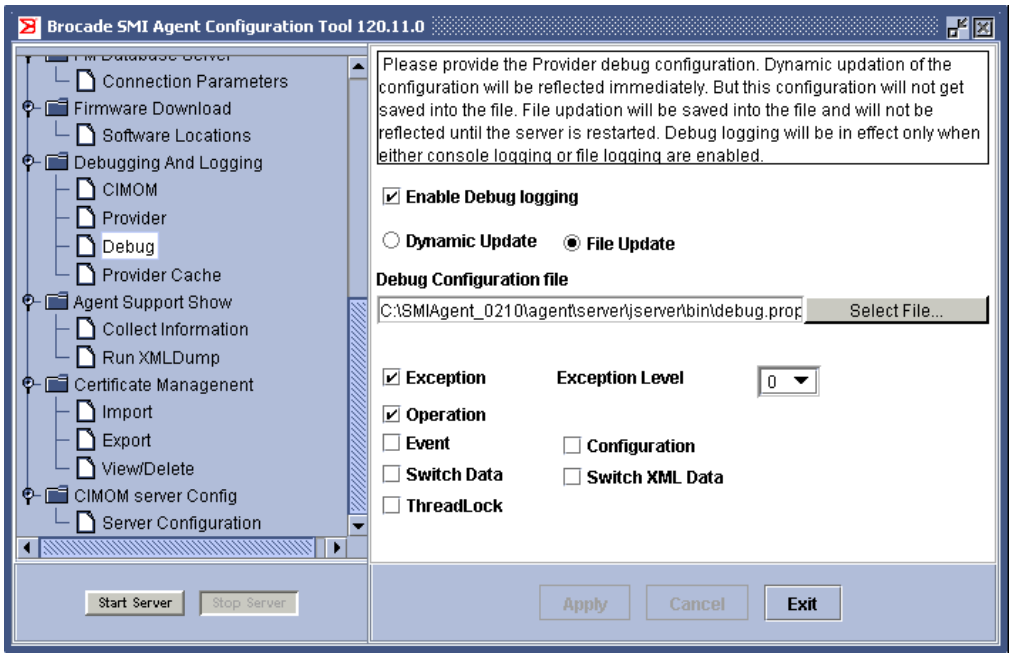


FIGURE 24 **Configure debugging options for provider**

Logging options for the provider

You can enable or disable console and file logging. When you enable file logging, you specify the location of the log file and optionally, the size and number of log files. If you specify the log file size and count, then when the specified size is exceeded on the first log file, logs will be written to the next log file.

Configuring logging options for provider

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Provider** in the menu tree (see Figure 25).

   The content pane displays the current logging configuration for the provider.
3. To enable console logging, check the **Enable Console logging** check box.
   To disable console logging, clear this box.

4. To enable file logging:
   a. Check the **Enable File logging** check box.
   b. Type the full path to the log file, or click **Select File** to browse for the file location.
   c. Type the size of the log file (in kilobytes). The log file size can be between 1 and 51200 kilobytes (between 1024 and 52428800 bytes).
   d. Type the number of log files.

   To disable file logging, clear the **Enable File logging** check box.
5. Click **Apply**.

The changes take effect when you restart the server. Click **Start Server** to restart the server.

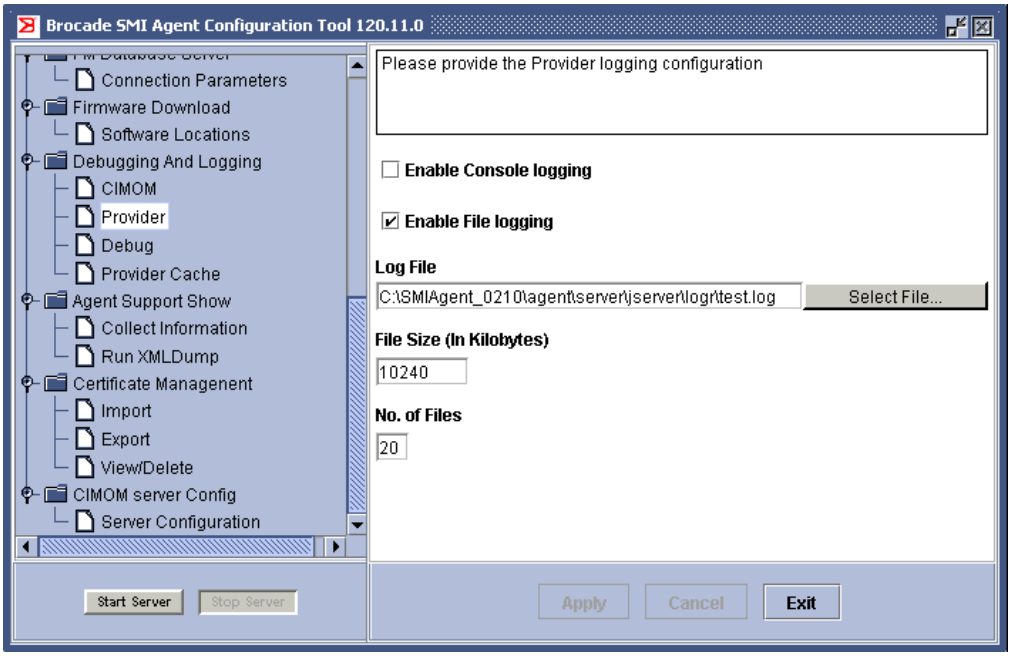


FIGURE 25 Configure logging options

Log file examples

The SMI-A trace information is appended to the log file each time the SMI-A is started. The following example shows the sample contents of the log file the first time the SMI-A is started:

```
<?xml version="1.0" encoding="windows=1252" standalone="no"?>
<!DOCTYPE log SYSTEM "logger.dtd">
<log>
<record>
.
.
.
</record>
</log>
```

The next example shows the contents of the log file on the subsequent startup. The text in bold is the contents from the second time the SMI-A was started.

```
<?xml version="1.0" encoding="windows=1252" standalone="no"?>
<!DOCTYPE log SYSTEM "logger.dtd">
<log>
<record>
.
.                 -------------> Contents from the first time run
.
</record>
</log>
<?xml version="1.0" encoding="windows=1252" standalone="no"?>
<!DOCTYPE log SYSTEM "logger.dtd">
<log>
<record>
.
.                 -------------> Contents from the second time run
.
</record>
</log>
```

Capture provider cache information

This section describes how you can write the dynamic information stored in the provider to a debug log file. The debug log file is an XML file.

Any of the following information can be logged:

- connection cache
- configuration
- zoning cache

The following procedure is the equivalent of the extrinsic method **Brocade_Agent.LogCacheData**.

Capturing information from the provider cache

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Provider Cache** in the menu tree (see Figure 26).
3. Check the check boxes next to the information you want to capture:
   - Connection Cache
   - Configuration
   - Zoning Cache
4. Type the location of the log file or click **Select Folder** to browse for the file location.

   An XML file with the name *SMIAgentCache<timestamp>* will be created in that location.
5. Click **Log Deadlock Information** to log the current status of threads that are in a deadlock situation.

   This is the equivalent of the extrinsic method **Brocade_Agent.LogCacheData**.
6. Click **Dump now**.

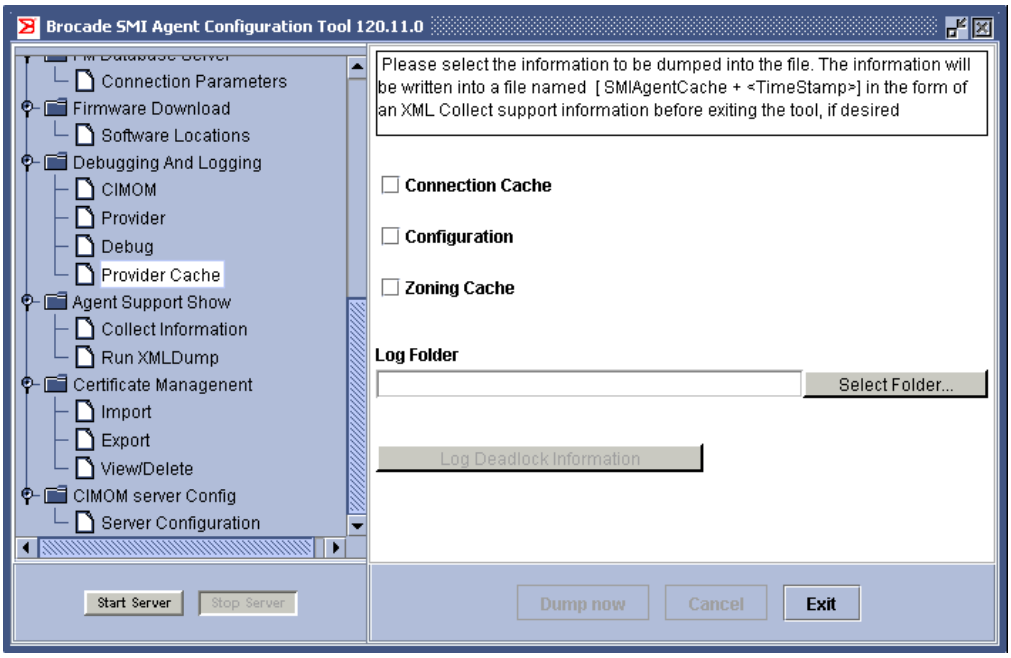


FIGURE 26 Configure provider cache

Support information collection

This section explains how to collect support information in case of any product-related issues.

- "Collect support information" on page 43
- "XML dump" on page 44

Collect support information

Use this procedure to collect all support information in one file. The required information is collected and zipped in a file named *SMISupportFiles.zip*. You can specify a location for this file, or use the default location:

On Linux, Solaris, and AIX:*<SMIAgent>/agent/SupportInfo*
On Windows: *<SMIAgent>\agent\SupportInfo*

where <SMIAgent> is the directory where the Brocade SMI Agent is installed.

The zip file contains the following files:

- *provider.xml*
- *jserver.properties*
- *SMIAgentconfig.xml*
- *cimom.properties*
- *SystemInfo.txt*
- CIMOM and provider log files, if any

Collecting support information

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Collect Information** in the menu tree (see Figure 27).

   The content pane displays the current path for the zip file.
3. To change the path of the zip file, type a new path or click **Select Folder** to browse for the location.
4. Click **Apply**.

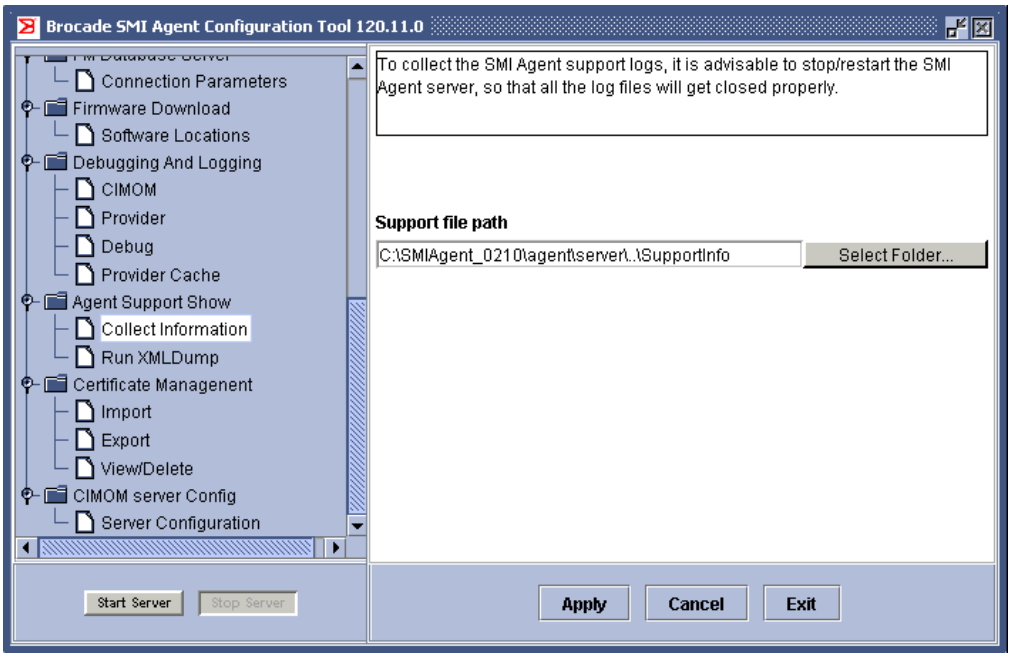


FIGURE 27 Collect support information

XML dump

An XML dump is a file that enumerates all instances of the leaf classes that have a provider support within all the namespaces in the SMI-A. Classes that represent indications (that have the "Indication" qualifier) are *not* included. The output is in CIM-XML format.

This procedure generates an XML dump for use in case of any product-related issues. To generate an XML dump, the SMI Agent server should be running.

Running an XML dump

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Run XML Dump** in the menu tree (see Figure 28 on page 45).

   The content pane displays the current path for the XML file.
3. To change the XML file path, type a new path or click **Select Folder** to browse for the location.
4. Click **Start Server** to ensure that the SMI Agent server is running.
5. Click **Apply**.

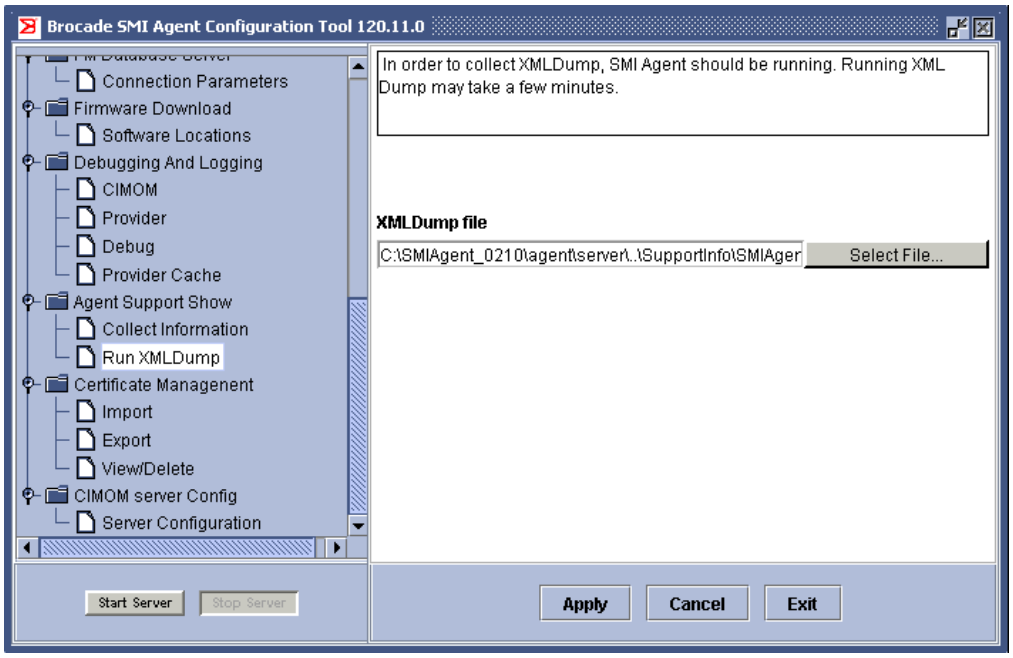


FIGURE 28 **Run XML dump**

CIMOM server configuration

If the server is running on a system using multiple IP addresses, the server binds to an IP address arbitrarily chosen by the underlying operating system. Using the following procedure, you can configure the server to use a specific IP address.

Configuring the CIMOM server

1. Launch the Brocade SMI Agent Configuration Tool.
2. Click **Server Configuration** in the menu tree (see Figure 29 on page 46).

   You must enable the stack before the SMI Agent can communicate using the IPv4 or IPv6 address.
3. Click **Enable** to enable the IPv4 stack, or click **Disable** to disable the IPv4 stack and use IPv6 instead.
4. Check the **Bind to Address** box to indicate the server should bind to a specific IP address, and enter the IP address (in IPv4 or IPv6 format) in the field.

   Clear the **Bind to Address**s box to indicate that the server should bind to an IP address that is arbitrarily chosen by the underlying operating system.
5. Click **Apply**.

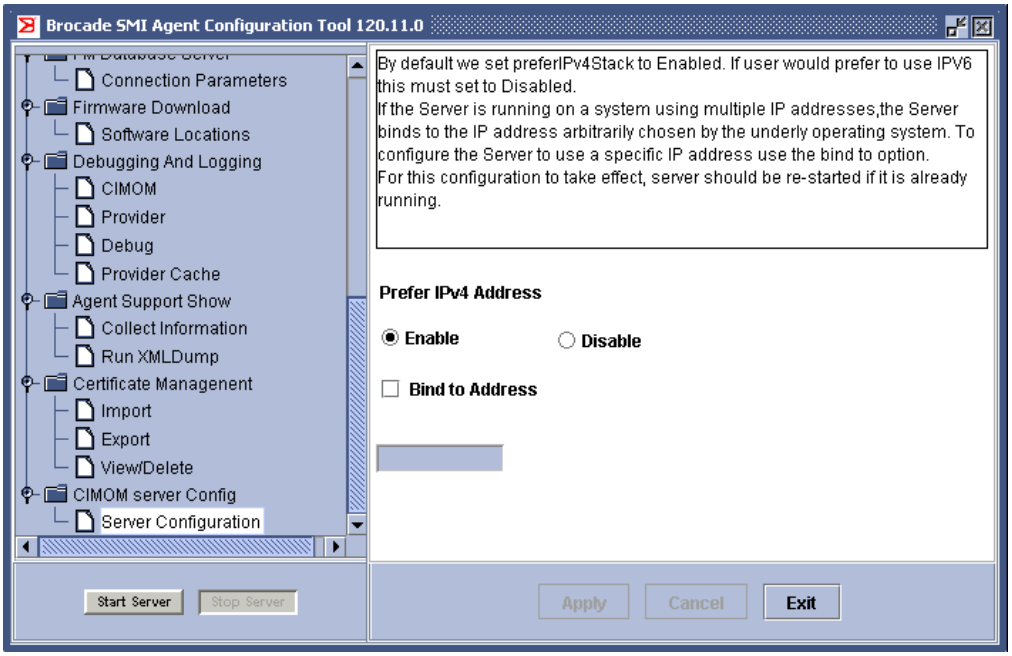


FIGURE 29 **Configure the CIMOM server**

Configuring log file options

You cannot configure log file options with the SMI Agent Configuration Tool. The following procedure describes how to change the log file options by modifying the *jserver.properties* file.

1. Open the *jserver.properties* file found at *...server/jserver/bin*.
2. Uncomment the following lines:

```
# com.wbemsolutions.jserver.logdirectory=/mylogfiledir
#com.wbemsolutions.jserver.log.maxfilesize=5000000
#com.wbemsolutions.jserver.log.numfiles=3
```

   Replace *mylogfiledir* with the complete path of the log file directory.

   Replace *5000000* with the maximum size of the log file (in KB).

   Replace *3* with the number of rotating log files.

When the specified size is exceeded on the first log file, logs are written to the next log file. When approximately the specified number of KB have been written to one log file, another log file is opened.

NOTE
Sometimes log file will exceed the size specified because of a limitation in Java logging. After the server is stopped, the size of the log file will be reduced to the size specified.

Chapter

Mutual Authentication for Clients and Indications 4

In this chapter

Introduction

The SMI-A installation wizard provides options for enabling mutual authentication for clients and indications. This chapter describes how you can enable mutual authentication *after* installation, without re-running the installation wizard.

If you enable mutual authentication, you should disable the CIM-XML client protocol adapter (CPA) for the SMI-A so that the clients can use only HTTPS communication. If you do not disable the CIM-XML CPA, then any client can communicate with the SMI-A using HTTP access.

The client and server certificates that are used in the mutual authentication are only private certificates that are generated by Brocade and are not verified by any certificate authority. Clients cannot add their own certificates to the server trust stores.

NOTE
Mutual authentication works using only Brocade-provided private certificates.

Mutual authentication for clients

You can restrict access to the SMI-A to only clients that are trusted by the agent. The SMI-A uses private key information and authentication information to allow only specific clients to send requests as SSL-encrypted CIM-XML to the SMI-A.

By default, mutual authentication for clients is disabled, which means that any client can use the HTTPS communication protocol to communicate with the SMI-A. When mutual authentication for clients is enabled, then only those clients whose certificates have been added to the SMI-A TrustStore can use HTTPS to communicate with the SMI-A. That is, the SMI-A must have a TrustStore that contains a certificate for an entry in the client KeyStore.

Additionally, when mutual authentication for clients is enabled, the client must have a TrustStore that contains the certificate for an entry in the SMI-A KeyStore.

Enabling mutual authentication for clients

1. Configure the SMI-A to support mutual authentication for clients. This can be done either during installation using the installation wizard, or after installation, as described in "Configuring mutual authentication for clients" on page 22.
2. Optionally, disable HTTP access so that only HTTPS access is available to the clients. HTTPS communication is preferred if mutual authentication is enabled. (See "Configuring HTTP access" on page 24.)
3. Optionally, configure the WBEM client to use client certificates to communicate with the SMI-A. (See "Client configuration to use client certificates" on page 48.)

Mutual authentication for indications

You can restrict delivery of indications using mutual SSL authentication to only clients that are trusted by the SMI-A.

By default, mutual authentication for indications is disabled, which means that the SMI-A uses SSL to send CIM-XML indications to a WBEM client listener, but does not attempt to verify the identity of the WBEM client listener. When mutual authentication for indications is enabled, then only those clients whose certificates have been added to the SMI-A Indications TrustStore can use SSL to receive indications from the SMI-A. That is, the SMI-A must have a TrustStore that contains a certificate for an entry in the client's Indications KeyStore.

Enabling mutual authentication for indications

1. Configure the SMI-A to support mutual authentication for indications. This can be done either during installation using the installation wizard, or after installation, as described in "Configuring mutual authentication for indications" on page 23.
2. Optionally, disable HTTP access so that only HTTPS access is available to the clients. HTTPS communication is preferred if mutual authentication is enabled. (See "Configuring HTTP access" on page 24.)
3. Optionally, configure the WBEM client to use client certificates to communicate with the SMI-A. (See "Client configuration to use client certificates," next.)

Client configuration to use client certificates

After installation is completed, the client certificates are in the following location:

On Linux, Solaris, and AIX:*<SMIAgent>/agent/client*

On Windows: *<SMIAgent>\agent\client*

This folder has the following files:

- *.client.keystore*
- *.client.truststore*
- *client.cer*
- *.client.ind.keystore*

- *.client.ind.truststore*
- *clientind.cer*

There are three ways to configure a WBEM client to use a client certificate with the SMI-A:

- using a property file
- using system property values when invoking the WBEM client
- using a WBEM client listener program (mutual authentication for indications only)

Configuring a client to use client certificates using a property file

1. Create a *WbemClient.properties* file, which contains information for the configuration of the client keystore and truststore.

   For example, if the SMI-A is installed under *D:\smiagent*, the contents of the *WbemClient.properties* file should be as follows.

   Mutual authentication for clients:

   ```
   javax.net.ssl.keyStore=D:/smiagent/agent/client/.client.keystore
   javax.net.ssl.keyStorePassword=SSLclient
   javax.net.ssl.trustStore=D:/smiagent/agent/client/.client.truststore
   javax.net.ssl.trustStorePassword=trustSSLclient
   ```

   Mutual authentication for indications:

   ```
   wbem.indications.keyStore=D:/smiagent/agent/client/.client.ind.keystore
   wbem.indications.keyStorePassword=SSLindication
   wbem.indications.trustStore=D:/smiagent/agent/client/.client.ind.truststore
   wbem.indications.trustStorePassword=trustSSLindication
   ```

   Note that both the javax.net.* properties and the wbem.indications.* properties can be specified in the same *WbemClient.properties* file.

2. Modify the CLASSPATH environment variable to reference this file.

   The CLASSPATH should contain only the path to the directory where the file is present and not the path to the file itself. For example, if the *WbemClient.properties* file is located at *C:\SMIAgent\agent*, then the CLASSPATH environment variable should be:

   C:\SMIAgent\agent

Configuring a client to use client certificates using system property values

Pass the required system properties as jvm parameters on the command line, using the -D option as follows.

Mutual authentication for clients:

```
java -classpath <SMIAgent>/agent/lib/wbem.jar
-Djavax.net.ssl.keyStore=<SMIAgent>/agent/client/.client.keystore
-Djavax.net.ssl.keyStorePassword=SSLclient
-Djavax.net.ssl.trustStore=<SMIAgent>/agent/client/.client.truststore
-Djavax.net.ssl.trustStorePassword=trustSSLclient
clientprogram
```

Mutual authentication for indications:

```
java -classpath <SMIAgent>/agent/wbem.jar
-Dwbem.indications.keyStore=<SMIAgent>/agent/client/.client.ind.keystore
-Dwbem.indications.keyStorePassword=SSLindication
-Dwbem.indications.trustStore=<SMIAgent>/agent/client/.client.ind.truststore
-Dwbem.indications.trustStorePassword=trustSSLindication
clientprogram
```

Configuring a client to use client certificates using client listener program (mutual authentication for indications only)

Set the required system properties within the client listener program. For example:

```
public class clientlistener {
private static final String KS = "indication.keyStore";
private static final String KSPWD = "indications.keyStorePassword";
private static final String TS = "indications.trustStore";
private static final String TSPWD = "indications.trustStorePassword";
System.setProperty(clientlistener.KS) =
"<SMIAgent>/agent/client/.client.ind.keystore";
System.setProperty(clientlistener.KSPWD) = "SSLindication";
System.setProperty(clientlistener.TS) =
"<SMIAgent>/agent/client/.client.ind.truststore";
System.setProperty(clientlistener.TSPWD) = "trustSSLindication";
}
```

Client configuration to use client certificates for default SSL indications

When mutual authentication for indications is *not* enabled, you can configure a client to use default SSL indications. There are three ways to configure a WBEM client to use default SSL indications:

- using a property file
- using system property values when invoking the WBEM client
- using a WBEM client listener program

The procedures are similar to those in "Client configuration to use client certificates" on page 48, the only difference being that you do *not* include the truststore information.

Note that the certificates installed for mutual authentication for clients and indications are not platform-specific. That is, the certificates installed for Windows, Linux, Solaris, and AIX are the same. Client certificates installed on one platform can be used by the clients running on other platforms.

Configuring a client for default SSL indications using a property file

1. Create a *WbemClient.properties* file, which contains information for the configuration of the client keystore. Do not include truststore information in the file.

   For example, if the SMI-A is installed under *D:\smiagent*, the contents of the *WbemClient.properties* file should be as follows.

   ```
   wbem.indications.keyStore=D:/smiagent/agent/client/.client.ind.keystore
   ```

```
wbem.indications.keyStorePassword=SSLindication
```

2. Modify the CLASSPATH environment variable to reference this file. The CLASSPATH should contain only the path to the directory where the file is present and not the path to the file itself. For example, if the *WbemClient.properties* file is located at *C:\SMIAgent\agent*, then the CLASSPATH environment variable should be:

   C:\SMIAgent\agent

Configuring a client for default SSL indications using system property values

Pass the required system properties as jvm parameters on the command line, using the -D option as follows.

```
java –classpath <SMIAgent>/agent/wbem.jar
-Dwbem.indications.keyStore=<SMIAgent>/agent/client/.client.ind.keystore
-Dwbem.indications.keyStorePassword=SSLindication
clientprogram
```

Do not pass the truststore information in the command line.

Configuring a client for default SSL indications using client listener program

Set the required system properties within the client listener program. For example:

```
public class clientlistener {
private static final String KS = "indication.keyStore";
private static final String KSPWD = "indications.keyStorePassword";
System.setProperty(clientlistener.KS) =
"<SMIAgent>/agent/client/.client.ind.keystore";
System.setProperty(clientlistener.KSPWD) = "SSLindication";
}
```

Do not include the truststore information in the client listener program.

Troubleshooting

If the keystore and truststore information is not set up correctly, the following errors are expected on the client side, depending on the WBEM client configuration:

- If the WBM client is configured with no keystore or truststore information, the following error is issued on the client side:

```
XMLERROR:
enumerateInstances,java.net.ConnectException: java.net.SocketException –
Software caused connection abort: recv failed
    at javax.wbem.client.adapter.http.CIMClientXML.enumerateInstances(Unknown
Source)
    at javax.wbem.client.CIMClient.enumerateInstances(Unknown Source)
    at javax.wbem.client.CIMClient.enumerateInstances(Unknown Source)
```

- If keystore or truststore information is not set up correctly, then the keystore and truststore information on the server does not correspond to the keystore and truststore information on the client. In this scenario, the following error is issued on the client side:

```
XMLERROR:
enumerateInstances,java.net.ConnectException:
javax.net.ssl.SSLHandshakeException - Received fatal alert: bad_certificate
    at javax.wbem.client.adapter.http.CIMClientXML.enumerateInstances(Unknown
Source)
    at javax.wbem.client.CIMClient.enumerateInstances(Unknown Source)
    at javax.wbem.client.CIMClient.enumerateInstances(Unknown Source)
```

Chapter

Frequently Asked Questions

5

In this chapter

General questions

Besides Windows Domain authentication, does the SMI Agent support local user authentication?

The SMI Agent also supports authenticating the user against the system on which it is installed. By default when you configure security, the user's credentials (username and password) are validated against the ones present on the local system. To ensure this happens, follow these steps:

1. During SMI-A installation, enable security and select "No" for Windows domain authentication.
2. Create a local user on the Windows system where the agent is installed.

What are some situations that might require restarting the SMI Agent?

Restarting of the SMIAgent is required when:

- configuration parameters, such as the debug level or log file name, are changed.
- host IP, HTTP, or HTTPS port is changed.
- firmware download configuration entry in *SMIAgentConfig.xml* is changed.

What are the Eventing and ARR TCP Ports? Do they relate to indications?

These are ports that are used by the agent to receive events and ARP responses from the fabric. The client is not required to fill in these ports; the operating system selects the ports dynamically. One probable use case for specifying these ports is if there is a firewall between the fabric and the host. In this case, you can specify a fixed port to be opened by the administrator for eventing or ARR.

If I have a firewall between the SMIAgent and the Brocade switch, what are the ports that must be opened and in which direction?

At login the Brocade SMI Agent first contacts the switch through RPC on portmapper port 111. All other calls to the switch are through RPC on ports 897 (non-secure) and 898 (secure).

The ARR and Eventing ports that you select are those on the Brocade SMI Agent host.

If there is a firewall between the Brocade SMI Agent and the Brocade fabric, the following ports must be opened:

SMIAgent to Switch:

- 111
- 897
- 898

Switch to SMIAgent:

- Your ARR and Eventing port selections

What encryption method is used to encrypt the password field in provider.xml?

The SMI Agent comes with a utility to encrypt the password. This utility is present in the following directory:

Linux, Solaris, and AIX:*<SMIAgent>/agent/bin/PasswordEncryptor*

Windows: *<SMIAgent>\agent\bin\PasswordEncryptor.bat*

Use this utility to encrypt the password.

How do I report a problem and what information should I provide?

Please fill in the “Submit Problem Report” form at the partner web site. See “Document feedback” on page xvi for additional information.

How do I collect diagnostic data from the Brocade SMI Agent?

The Brocade SMI Agent Configuration Tool (described in this document) can be used to collect required data.

Does the Brocade SMI Agent need to point to every switch in a fabric or just one switch in each fabric to collect the data?

Just one switch per fabric.

Can the SMI Agent proxy for two fabrics that are in different subnets?

Yes.

Should I designate multiple proxies into a fabric? What are the best practices concerning this?

You can have only one connection at a time into the fabric. The only advantage in designating multiple proxies is that if the first proxy fails to connect, the SMI-A tries the next proxy until it finds one that works.

Do the start_server and stop_server scripts work if the agent is set to run as a daemon on Linux and Solaris? Do these scripts work if the agent running as a service on Windows or do you have to use the Services window?

If the agent is set to run as a daemon on Linux, Solaris, and AIX, or as a service on Windows. use the start_agent_service and stop_agent_service scripts instead. On Windows, you can also use the Services window.

On Linux, Solaris, and AIX, you must have root permissions to stop the service.

The best way to start and stop the server is to use the Configuration Tool.

In using Windows domain authentication, do I need to include the domain name along with the username for authentication?

No. You should provide only the username, as shown:

```
UserPrincipal up = new UserPrincipal("username");
PasswordCredential pc = new PasswordCredential("password");
```

Does the SMI Agent have support for HTTPS communication?

Yes, the SMI Agent supports HTTPS (the combination of a normal HTTP interaction over an encrypted secure socket layer (SSL) or transport layer security (TLS) transport mechanism) between the CIMClient and SMI Agent. The Brocade SMI Agent also supports secure communication between the SMI Agent and the fabric via secure RPC.

Does the SMI Agent work on hosts with multiple IP addresses? If so is there a way to configure the CIMOM to choose a specific NIC/IP? Is there anything special I need to do for the SMI Agent to see proxy switches connected to the second NIC, or will it just work by default?

Starting with 120.6.0 the Brocade SMI Agent supports multi-homed hosts. Some systems have multiple network interfaces that are connected to different IP subnets. Each connection uses a different IP address. By default, the CIMOM uses all IP addresses used by the system. To configure the CIMOM to use only a specific IP address, modify the *jserver.properties* file found at *.../server/jserver/bin* with the following entry:

```
HostIPAddress=<specific ip address>
```

This forces the CIMOM to only use the network interface with <specific IP address> even though the system uses other network interfaces with different IP addresses.

To configure the IP address for Switch-to-SMIAgent communication in multi-homed systems, see "Enable multi-homed support" on page 12.

How do I tell what version of SMI-A I am running?

The title bar in the Brocade SMI Agent Configuration Tool displays the version of the SMI-A, for versions 120.7.0 and later. See Figure 3 on page 14 for an example.

Troubleshooting

How do I prevent the SMI Agent process from getting terminated on Solaris when I start the agent in a Bourne shell and then log out?

When you starts the agent in a Bourne shell (*/bin/sh*), the process dies upon user session logout. To prevent this, start the SMI Agent using the following command:

/usr/bin/nohup start_server

Note that in the C shell, background jobs are by default immune to being killed by a shell exit.

If the Brocade SMI Agent hangs, how do I capture the thread dump?

On Linux: Type the following command:

```
kill -3 pid
```

where *pid* is the process ID of the Brocade SMI Agent.

On Solaris: Press CTRL key + backslash (\) key.

On Windows: Press CTRL key + BREAK key.

Why is there no change in the status of a non-proxy Brocade_Switch when a LAN cable from the non-proxy switch is unplugged?

Communication from proxy to target switches is in-band. So even if the LAN cable from a non-proxy switch is unplugged, the agent can still talk to that target switch via the fibre connecting this proxy switch and the non-proxy switch.

The Brocade SMI Agent does not send out any alerts for this.

What does the error message "Host Message: Duplicate connection to fabric ...." mean?

This is an informative error message that occurs when the *provider.xml* file is configured with IP addresses of different switches in the same fabric. The Brocade SMI Agent tries to connect to each entry in the *provider.xml* file. If a connection to the fabric already exists, then this message occurs. Only one switch entry per fabric is sufficient in the *provider.xml* file.

Appendix

Licenses and Attributions

A

In this chapter

Open source software used in SMI-A

The CIM MOF files used with the SMI-A are used with the permission of the Distributed Management Task force (DMTF) and are copyrighted by the DMTF.

Some components of the SMI-A are derived from open source software. For your convenience the licenses are included in this document as well as installed as part of the release.

- WBEM Services open source project (Sun Industry Standards Source License)

  The JavaTM WBEM API, J WBEM Server and MOF Compiler are derived from the WBEM Services open source project. The license for WBEM Services is the Sun Industry Standards Source License (SISSL) – section 13.1. For more information on WBEM Services see

  http://wbemservices.sourceforge.net/

- Standards Based Linux Instrumentation for Manageability (IBM Common Public License)

  The Native Provider Interface (NPI) Provider Protocol Adapter is based on work done in SBLIM (pronounced “sublime”). The Standards Based Linux Instrumentation for Manageability is an IBM Open Source project, intended to enhance the manageability of GNU/Linux systems. The license for SBLIM is the IBM Common Public License. For more information on SBLIM, see

  http://www-124.ibm.com/sblim/

- SLP (OpenSLP License)

  The SLP implementation uses the openSLP implementation and its license is a BSD style license. For more information on openSLP, see

  http://www.openslp.org

- Cryptography Security Library, version 1.19 (Bouncy Castle)

  The SMI Agent uses only the RSA algorithm. For more information on The Legion Of The Bouncy Castle, see *http://www.bouncycastle.org*

- Remotetea (ONC RPC), version 1.0.1 (GNU Library General Public License)
- util.concurrent package, release 1.3.4 (Public Domain)
- SUN J2SDK, version 1.4.2_x (Sun Binary Code License Agreement)

Sun Industry Standards Source License

Sun Industry Standards Source License - Version 1.2

1.1 "Commercial Use" means distribution or otherwise making the Original Code available to a third party.

1.2 "Contributor Version" means the combination of the Original Code, and the Modifications made by that particular Contributor.

1.3 "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.4 "Executable" means Original Code in any form other than Source Code.

1.5 "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.6 "Larger Work" means a work which combines Original Code or portions thereof with code not governed by the terms of this License.

1.7 "License" means this document.

1.8 "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9 "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. A Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10 "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code.

1.11 "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.12 "Source Code" means the preferred form of the Original Code for making modifications to it, including all modules it contains, plus any associated interface definition files, or scripts used to control compilation and installation of an Executable.

1.13 "Standards" means the standards identified in Exhibit B.

1.14 "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You'' includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control'' means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2.0 SOURCE CODE LICENSE

2.1 The Initial Developer Grant

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices, including but not limited to Modifications.

3.0 DISTRIBUTION OBLIGATIONS

3.1 Application of License.

The Source Code version of Original Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. Your license for shipment of the Contributor Version is conditioned upon Your full compliance with this Section. The Modifications which You create must comply with all requirements set out by the Standards body in effect one hundred twenty (120) days before You ship the Contributor Version. In the event that the Modifications do not meet such requirements, You agree to publish either (i) any deviation from the Standards protocol resulting from implementation of Your Modifications and a reference implementation of Your Modifications or (ii) Your Modifications in Source Code form, and to make any such deviation and reference implementation or Modifications available to all third parties under the same terms as this license on a royalty free basis within thirty (30) days of Your first customer shipment of Your Modifications. Additionally, in the event that the Modifications you create do not meet the requirements set out in this Section, You agree to comply with the Standards requirements set out in Exhibit B.

3.2 Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add Your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Initial Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Your version of the Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer for any liability incurred by the Initial Developer as a result of warranty, support, indemnity or liability terms You offer.

3.3 Distribution of Executable Versions.

You may distribute Original Code in Executable and Source form only if the requirements of Sections 3.1 and 3.2 have been met for that Original Code, and if You include a notice stating that the Source Code version of the Original Code is available under the terms of this License. The notice must be conspicuously included in any notice in an Executable or Source versions, related documentation or collateral in which You describe recipients' rights relating to the Original Code. You may distribute the Executable and Source versions of Your version of the Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License. If You distribute the Executable and Source versions under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer. You hereby agree to indemnify the Initial Developer for any liability incurred by the Initial Developer as a result of any such terms You offer.

3.4 Larger Works.

You may create a Larger Work by combining Original Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Original Code.

4.0 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Original Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.2 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5.0 APPLICATION OF THIS LICENSE

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Modifications as set out in Section 3.1.

6.0 VERSIONS OF THE LICENSE

6.1 New Versions.

Initial Developer may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2 Effect of New Versions.

Once Original Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Original Code under the terms of any subsequent version of the License published by Initial Developer. No one other than Initial Developer has the right to modify the terms applicable to Original Code.

7.0 DISCLAIMER OF WARRANTY

ORIGINAL CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE ORIGINAL CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE ORIGINAL CODE IS WITH YOU. SHOULD ANY ORIGINAL CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY ORIGINAL CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8.0 TERMINATION

8.1 This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Original Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2 In the event of termination under Section 8.1 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9.0 LIMIT OF LIABILITY

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF ORIGINAL CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10.0 U.S. GOVERNMENT END USERS

U.S. Government: If this Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in the Software and accompanying documentation shall be only as set forth in this license; this is in accordance with 48 C.F.R. 227.7201 through 227.7202-4 (for Department of Defense (DoD) acquisitions) and with 48 C.F.R. 2.101 and 12.212 (for non-DoD acquisitions).

11.0 MISCELLANEOUS

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to any litigation relating to this License, the losing party shall be responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

EXHIBIT A - Sun Industry Standards Source License (SISSL)

"The contents of this file are subject to the Sun Industry Standards Source License Version 1.2 (the "License"); You may not use this file except in compliance with the License. You may obtain a copy of the License at http://wbemservices.sourceforge.net/license.html

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is WBEM Services.

The Initial Developer of the Original Code is: Sun Microsystems, Inc.

Portions created by: Sun Microsystems, Inc. are Copyright © 2001 Sun Microsystems, Inc. All Rights Reserved.

Contributor(s): _____

EXHIBIT B - Standards

The Standard is defined as the following:

CIM Specification v2.2

XML Mapping Specifications v2.0.0

CIM Operations over HTTP v1.0

WBEM Services Specification 1.0 as defined pursuant to the JCP 2.0 (http://java.sun.com/aboutJava/communityprocess/jcp2.html)

Naming Conventions: If any of your Modifications do not meet the requirements of the Standard, then you must change the package names and public class and interface declarations of the work created by the Original Code plus your Modifications so that java.*, javax.* com.sun.* and similar naming conventions are not used. Also, if any of your Modifications do not meet the requirements of the Standard you may not claim, directly or indirectly, that your implementation of the Standard is compliant.

IBM Common Public License

Common Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a nonexclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a nonexclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

OpenSLP License

The following copyright and license is applicable to the entire OpenSLP project (libslp, slpd, and related documentation):

Copyright (C) 2000 Caldera Systems, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Caldera Systems nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CALDERA SYSTEMS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bouncy Castle

Copyright (c) 2000 - 2006 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GNU Library General Public License

Copyright (c) 1999, 2000

Lehrstuhl fuer Prozessleittechnik (PLT), RWTH Aachen

D-52064 Aachen, Germany.

All rights reserved.

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this program (see the file COPYING.LIB for more details); if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Public Domain

Originally written by Doug Lea and released into the public domain. This may be used for any purposes whatsoever without acknowledgment. Thanks for the assistance and support of Sun Microsystems Labs, and everyone contributing, testing, and using this code.

Sun Binary Code License Agreement

Sun Microsystems, Inc.

Binary Code License Agreement

for the

JAVATM 2 SOFTWARE DEVELOPMENT KIT (J2SDK),

STANDARD EDITION, VERSION 1.4.2_X

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1.DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java 2 Platform, Standard Edition (J2SETM platform) platform on Java-enabled general purpose desktop computers and servers.

2.LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3.RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. Licensee acknowledges that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4.LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited

warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5.DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6.LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7.SOFTWARE UPDATES FROM SUN. You acknowledge that at your request or consent optional features of the Software may download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

8.SOFTWARE FROM SOURCES OTHER THAN SUN. You acknowledge that, by your use of optional features of the Software and/or by requesting services that require use of the optional features of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

9.TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

10.EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

11.TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

12.U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13.GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

15. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A.Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B.License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C.License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (v) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D.Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E.Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Software Development Kit, Standard Edition, Version 1.4.2; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2003, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the

Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (i) provides you prompt notice of the claim; (ii) gives you sole control of the defense and settlement of the claim; (iii) provides you, at your expense, with all available information, assistance and authority to defend; and (iv) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A, Attention: Contracts Administration.

F.Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G.Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#129530/Form ID#011801)

A Sun Binary Code License Agreement

Index

M

P

S

U

W

X