Brocade SMI Agent

Installation Guide

Supporting SMI Agent v110.5.0

Publication Number: 53-1000198-01
Publication Date: 11/30/06

 Publication Number: 53-1000198-01

Brocade Communications Systems, Incorporated

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

European and Latin American Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour A - 2ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 56 40
Fax: +41 22 799 56 41
Email: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Singapore Pte. Ltd.
9 Raffles Place
#59-02 Republic Plaza 1
Singapore 048619
Tel: +65-6538-4700
Fax: +65-6538-0302
Email: apac-info@brocade.com

Document History

The following table lists all versions of the *Brocade SMI Agent Installation Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Brocade SMI Agent Installation Guide	53-1000054-01	This is the first release of this book.	April 2006
Brocade SMI Agent Installation Guide	53-1000054-02	Removed VM directory from CD image path.	May 2006
Brocade SMI Agent Installation Guide	53-1000198-01	Updated to support the 110.5.0 release.	November 2006

Contents

About This Document

How This Document Is Organized v
What's New in this Document v
Supported Hardware and Software vi
Document Conventions vi
Text Formatting vi
Notes, Cautions, and Warnings vii
Key Terms vii
Additional Information vii
Brocade Resources vii
Other Industry Resources x
Getting Technical Help x
Brocade SMI Agent Support xi
Document Feedback xii

Chapter 1 Installation Requirements

Platform Requirements 1-1
Switch Requirements 1-1
System Requirements 1-2

Chapter 2 Installing the SMI Agent

Introduction 2-1
Before Installing the SMI Agent on Linux and Solaris 2-1
Installing the Brocade SMI Agent Using the Wizard 2-2
Installing the Brocade SMI Agent in Silent Mode 2-19
Creating a Properties File for Silent Installation 2-19
Triggering Silent Mode Installation 2-22

Post-Installation Considerations 2-23
Uninstalling the Brocade SMI Agent 2-23

Chapter 3 Silent Installation Status Messages

Chapter 4 Frequently Asked Questions

Index

About This Document

This document is an installation guide written for users who need to install the Brocade SMI Agent.

"About This Document" contains the following sections:

- "How This Document Is Organized," next
- "What's New in this Document" on page v
- "Supported Hardware and Software" on page vi
- "Document Conventions" on page vi
- "Additional Information" on page vii
- "Getting Technical Help" on page x
- "Brocade SMI Agent Support" on page xi
- "Document Feedback" on page xii

How This Document Is Organized

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, "Installation Requirements" lists the memory requirements and supported platforms for the Brocade SMI Agent.
- Chapter 2, "Installing the SMI Agent" explains how to install and uninstall the Brocade SMI Agent.
- Chapter 3, "Silent Installation Status Messages" lists the status messages that you might encounter when performing a silent installation of the Brocade SMI Agent.
- Chapter 4, "Frequently Asked Questions" provides answers to the most frequently asked questions sent to the SMI Agent Developer Support email address.

What's New in this Document

- The installation procedures for Linux, Solaris, and Windows, are combined into one procedure for Wizard installation and one procedure for silent mode installation.
- Screen shots of every installation screen are included.
- Secure eventing and ARR ports are supported.
- A new chapter for Frequently Asked Questions (FAQs) is added.

Supported Hardware and Software

The following switches are supported by Brocade SMI Agent 110.5.0:

- Brocade SilkWorm 200E switch
- Brocade SilkWorm 3000 switch
- Brocade SilkWorm 3014 switch
- Brocade SilkWorm 3016 switch
- Brocade SilkWorm 3200 switch
- Brocade SilkWorm 3250 switch
- Brocade SilkWorm 3800 switch
- Brocade SilkWorm 3850 switch
- Brocade SilkWorm 3900 switch
- Brocade SilkWorm 4012 switch
- Brocade SilkWorm 4020 switch
- Brocade SilkWorm 4100 switch
- Brocade SilkWorm 4900 switch
- Brocade SilkWorm 7500 switch
- Brocade SilkWorm 12000 director
- Brocade SilkWorm 24000 director
- Brocade SilkWorm 48000 director
- Brocade SilkWorm Multiprotocol Router Model AP7420

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for SMI-A 110.5.0, documenting all possible configurations and scenarios is beyond the scope of this document.

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.

Document Conventions

This section describes text formatting conventions and important notices formats.

Text Formatting

The narrative-text formatting conventions that are used in this document 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 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 appear in this document.

Note
A note provides a tip, emphasizes important information, or provides a reference to related information.

Caution
A caution alerts you to potential damage to hardware, firmware, software, or data.

Warning
A warning alerts you to potential danger to personnel.

Key Terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary.*

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

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

Additional Information

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

Brocade Resources

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

SMI-A

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

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.

Note

Go to *http://www.brocade.com* and click **Brocade Connect** to register at no cost for a user ID and password.

Fabric OS

- *Fabric OS Administrator's Guide*
- *Fabric OS Command Reference Manual*
- *Fabric OS MIB Reference Manual*
- *Fabric OS System Error Message Reference Manual*
- *Brocade Glossary*

XPath OS

- *XPath OS Administrator's Guide*
- *XPath OS Command Reference Manual*
- *XPath OS MIB Reference Manual*
- *XPath OS System Error Message Reference Manual*
- *Web Tools—AP Edition Administrator's Guide*

Optional Applications

- *Web Tools Administrator's Guide*
- *Fabric Watch Administrator's Guide*
- *Fabric Manager Administrator's Guide*
- *Secure Fabric OS Administrator's Guide*
- *EZSwitchSetup Administrator's Guide*

SilkWorm 48000

- *SilkWorm 48000 Hardware Reference Manual*
- *SilkWorm 48000 QuickStart Guide*
- *FR4-18i Hardware Reference Manual*
- *FR4-16IP Hardware Reference Manual*

SilkWorm 24000

- *SilkWorm 24000 Hardware Reference Manual*
- *SilkWorm 24000 QuickStart Guide*

SilkWorm 24000/48000

- *Port Blade and Filler Panel Replacement Procedure*
- *Control Processor Blade Replacement Procedure*
- *Blower Assembly Replacement Procedure*

- *Cable Management Tray and Guide Replacement Procedure*
- *Chassis Door Replacement Procedure*
- *WWN Bezel and Card Replacement Procedure*
- *Power Supply and Filler Panel Replacement Procedure*
- *14U Rack Mount Kit Installation Procedure*
- *Mid-Mount Rack Kit Installation Procedure*

SilkWorm 7500

- *SilkWorm 7500 Hardware Reference Manual*
- *SilkWorm 7500 QuickStart Guide*
- *SilkWorm 7500 Fan Assembly Replacement Procedure*
- *SilkWorm Mid Sized Power Supply Replacement Procedure*

SilkWorm 4900

- *SilkWorm 4900 Hardware Reference Manual*
- *SilkWorm 4900 QuickStart Guide*
- *SilkWorm 4900 Fan Assembly Replacement Procedure*
- *SilkWorm Mid Sized Power Supply Replacement Procedure*

SilkWorm 4100

- *SilkWorm 4100 Hardware Reference Manual*
- *SilkWorm 4100 QuickStart Guide*

SilkWorm 3900

- *SilkWorm 3900 Hardware Reference Manual* (for v4.x software)
- *SilkWorm 3900 QuickStart Guide* (for v4.x software)
- *SilkWorm 3900 Fan Assembly Replacement Procedure*
- *SilkWorm 3900 Motherboard Assembly Replacement Procedure*
- *SilkWorm 3900 Power Supply Replacement Procedure*

SilkWorm 3250/3850

- *SilkWorm 3250/3850 Hardware Reference Manual* (for v4.x software)
- *SilkWorm 3250/3850 QuickStart Guide* (for v4.x software)

SilkWorm 3016

- *SilkWorm 3016 Hardware Reference Manual* (for v4.2.x and later software)
- *SilkWorm 3016 QuickStart Guide* (for v4.2.x and later software)
- *Brocade Enterprise and Entry SAN Switch Modules for IBM eServer BladeCenter Design, Deployment and Management Guide* (DDM)

SilkWorm 3014

- *SilkWorm 3014 Hardware Reference Manual* (for v5.x software)
- *SilkWorm 3014 QuickStart Guide* (for v5.x software)

SilkWorm 200E

- *SilkWorm 200E Hardware Reference Manual* (for v5.x software)

SilkWorm Multiprotocol Router Model AP7420

- *SilkWorm Multiprotocol Router Model AP7420 Hardware Reference Manual*
- *SilkWorm Multiprotocol Router Model AP7420 QuickStart Guide*
- *SilkWorm Multiprotocol Router Model AP7420 Power Supply Replacement Procedure*
- *SilkWorm Multiprotocol Router Model AP7420 Fan Assembly Replacement Procedure*

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 SAN Info Center and click the Resource Library location:

http://www.brocade.com

Release notes are available on the Brocade Connect 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, as well as other applications:

http://www.t11.org

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

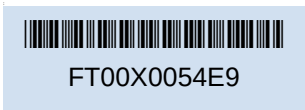
http://www.fibrechannel.org

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**
   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem and specific questions
   - Description of any troubleshooting steps already performed and 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 shown here:

   The serial number label is located as follows:
   - *SilkWorm 3014*—On the top of the chassis, under the insertion arm
   - *SilkWorm 3016 and 4012*—On the bottom of the switch module
   - *SilkWorm 200E, 3200, 3250 and 3850*—On the bottom of the chassis
   - *SilkWorm 3800 and 3900*— Nonport side of the chassis
   - *SilkWorm 4100, 4900, and 7500*—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - *SilkWorm 12000, 24000, and 48000*—Inside the chassis next to the power supply bays
   - *SilkWorm Multiprotocol Router Model AP7420*—On the bottom of the chassis and on the back of the chassis.
3. **World Wide Name (WWN)**
   - *SilkWorm 200E, 3014, 3016, 3250, 3850, 3900, 4012, 4100, 4900, 7500 switches and SilkWorm 24000, and 48000 directors:* Provide the license ID. Use the **licenseIDShow** command to display the license ID.
   - *SilkWorm Multiprotocol Router Model AP7420:* Provide the switch WWN. Use the **switchShow** command to display the switch WWN.
   - *All other SilkWorm switches:* Provide the switch WWN. Use the **wwn** 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:

SMIADevSup@brocade.com

When contacting developer 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

You can use the SMI Agent Configuration Tool to collect the required support information to be sent. Refer to the *Brocade SMI Agent User's Guide* for information about this tool.

Send ideas or requests for new Brocade SMI Agent features or enhancements to:

SMIADevSup@brocade.com

For general how-to answers about the telnet interface or the hardware, contact:

support@brocade.com

Document Feedback

Because quality is our first concern at Brocade, 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 and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Installation Requirements

Chapter 1

This chapter contains the following sections:

- "Platform Requirements" on page 1-1
- "Switch Requirements" on page 1-1
- "System Requirements" on page 1-2

Platform Requirements

Your software environment must meet the following requirements before you install the Brocade SMI Agent (SMI-A):

- Minimum of 512 MB RAM
- One of the following operating systems (32-bit versions only):
  - Microsoft Windows 2000 Professional or Windows Server 2003
  - Sun Solaris version 8, 9, or 10
  - Linux Red Hat AS 3.0 or Suse 9.1 Professional
- For Linux and Solaris, a graphical interface is required for standard installation, but not for silent installation.

Sun Microsystems JRE version 1.4.2_11 is bundled with the SMI-A and is automatically installed when the SMI-A is installed. (Note that SMI-A 110.5.0 is not compatible with JDK 1.5.)

Switch Requirements

When possible, you should upgrade your switches to Fabric OS v5.2.0 or higher. In particular, the proxy switch should be running Fabric OS 5.2.0 or higher.

The SMI-A does not support Fabric OS v2.6.x and v3.0.x switches as proxy switches.

It is not necessary to choose the principal switch as the proxy.

Only fabrics in which all user accounts are equivalent on all switches have been tested. For Admin Domains and RBAC, only fabrics containing all Fabric OS 5.2.0 switches have been tested.

System Requirements

Table 1-1 lists the memory and CPU recommendations.

Table 1-1 System Requirements

Requirements	SAN with 1-5,000 Switch Ports	SAN with 5,000-10,000 Switch Ports
Memory usage by the Agent	less than 512 MB	less than 1 GB
Memory	2 GB	3 GB
CPU	3 GHz	3 GHz

The memory required for running the SMI-A depends on the following:

- number of switches
- number of ports
- number of devices in a single fabric
- number of fabrics being managed

You should increase the memory as these numbers increase. You should also check the memory usage of all applications and services running on the host and adjust the memory accordingly. If the agent is used to manage multiple fabrics, use the total number of switch ports in all fabrics to determine the memory usage.

For the 110.5.0 release, SMI-A has been tested in a fabric with more than 3700 switch ports and more than 2000 devices. The memory usage in such fabric is less than 350 MB. The SMI-A has also been tested in a fabric with more than 11,000 simulated switch ports. The memory usage is less than 700 MB.

You should also increase the memory heap size for the JVM based on the number of switches and number of switch ports and devices. After you install the SMI Agent, you can increase the memory size or heap size using the following procedure.

Note

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

To increase the memory size or heap size

1. If you installed the SMI-A as a service on Windows, open the *jserverd.ini* file for editing. This file is in the following location:

   C:\Windows\system32\jserverd.ini

   If you did not install the SMI-A as a service, open the *start_server* file for editing:

   Linux and Solaris: <*SMIAgent*>*/agent/server/jserver/bin/start_server*
   Windows: <*SMIAgent*>*\agent\server\jserver\bin\start_server.bat*

2. Modify the JVM flag in the file.

   The default value of the JVM flag is: -Xmx512m. For example, to increase the memory from 512 MB to 1024 MB, change this value to: -Xmx1024m

   For most fabrics, 512 MB is usually sufficient.

3. Restart the SMI Agent, if it is already started.

Installing the SMI Agent

Chapter 2

This chapter contains the following information:

- "Introduction" on page 2-1
- "Before Installing the SMI Agent on Linux and Solaris" on page 2-1
- "Installing the Brocade SMI Agent Using the Wizard" on page 2-2
- "Installing the Brocade SMI Agent in Silent Mode" on page 2-19
- "Post-Installation Considerations" on page 2-23
- "Uninstalling the Brocade SMI Agent" on page 2-23

Introduction

This chapter describes the steps for installing and uninstalling the Brocade SMI Agent (SMI-A) on Windows, Linux, and Solaris. You can install the SMI-A either using a wizard or in silent mode, with no user intervention. The SMI-A does not support upgrades. You should first uninstall the SMI-A and then install the new version.

When SMI-A installation is complete, the following shortcuts are automatically added to the Start menu:

- Start CIMOM
- Stop CIMOM
- Start SMI Agent Service (*Available only if the* SMI-A *is installed as a service*)
- Stop SMI Agent Service (*Available only if the* SMI-A *is installed as a service*)
- Uninstall Brocade SMI Agent

Before Installing the SMI Agent on Linux and Solaris

The installation wizard allows you to install the SMI-A as a service on Windows, Linux, and Solaris. On Linux and Solaris, if the SMI-A is already installed and running as a service, then use the following procedure before starting a new installation for running SMI-A as a service.

1. Go to the previously installed *<SMIAgent>/agent/server/jserver/bin* directory.
2. Edit the **stop_agent_service** script in that directory according to the instructions given in the script.
3. Stop the service using the **stop_agent_service** script.
4. Start the new SMI-A installation, as described in "Installing the Brocade SMI Agent Using the Wizard," next, or "Installing the Brocade SMI Agent in Silent Mode" on page 2-19.

Installing the Brocade SMI Agent Using the Wizard

An installation wizard is provided for installing the SMI-A. The installation wizard does the following:

- installs Sun Microsystems JRE 1.4.2_11, which is bundled with the installer. The JRE is installed in the directory local to <*SMIAgent*>.
- allows you to configure Fabric Manager database server information (*SMIAgentConfig.xml* file)
- provides option for enabling security for the SMI-A.
  - During Windows installation, if security is enabled *with* Windows Domain Authentication, you must always provide the Windows Domain login credentials to connect to the SMI Agent; otherwise, all communication to the SMI-A will fail.
  - If security is enabled *without* Windows Domain Authentication, you must always provide the local account credentials to connect to the SMI Agent; otherwise, all communication to the SMI-A will fail.
  - During Linux and Solaris installations, if security is enabled during installation, then you must always start the SMI-A as root; otherwise, all communication to the SMI-A will fail.
- provides options for enabling mutual authentication for client and indications.
- allows you to configure http and https port information.
- allows you to configure eventing and ARR TCP ports (*SMIAgentConfig.xml* file)
- allows you to configure secure eventing and ARR TCP ports (*SMIAgentConfig.xml* file)
- provides options for enabling console and file logging (*start_server* file)
- allows you to configure proxy connections (*provider.xml* file)
- provides option for starting the SMI-A as a Windows service or Linux/Solaris daemon.
- installs the Brocade SMI Agent Configuration Tool, which allows you to change the SMI-A configuration settings after the installation. Refer to the *Brocade SMI Agent User's Guide* for information about the Configuration Tool.

To install the SMI-A using the wizard

1. Locate the installation file for the computer you are installing it on, as follows:
   - Windows: *CD_Image\Windows\install.exe*
   - Linux: *CD_Image\Linux\install.bin*
   - Solaris: *CD_Image\Solaris\install.bin*
2. Run the installation file.

Note

To enable security on Linux, you must start the installation process by logging in as root.

The installation wizard launches, as shown in Figure 2-1.

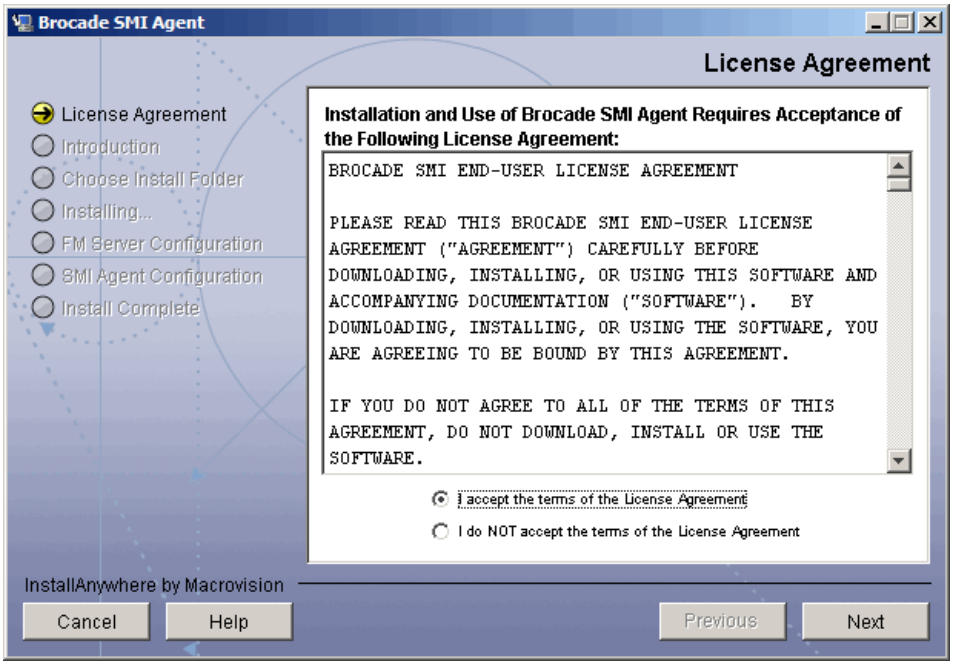


Figure 2-1 Installation Wizard

If the installation wizard does not launch, you might be installing in silent mode. Silent mode is triggered by the presence of a file named *installer.properties* in the same folder as *install.exe*. Check for the presence of the *installer.properties* file and, if you do not want to install in silent mode, either move that file to another folder, or rename the file. "Installing the Brocade SMI Agent in Silent Mode" on page 2-19 contains information about silent mode installation.

3. Accept the license agreement and click **Next**.

The System Configuration window appears.

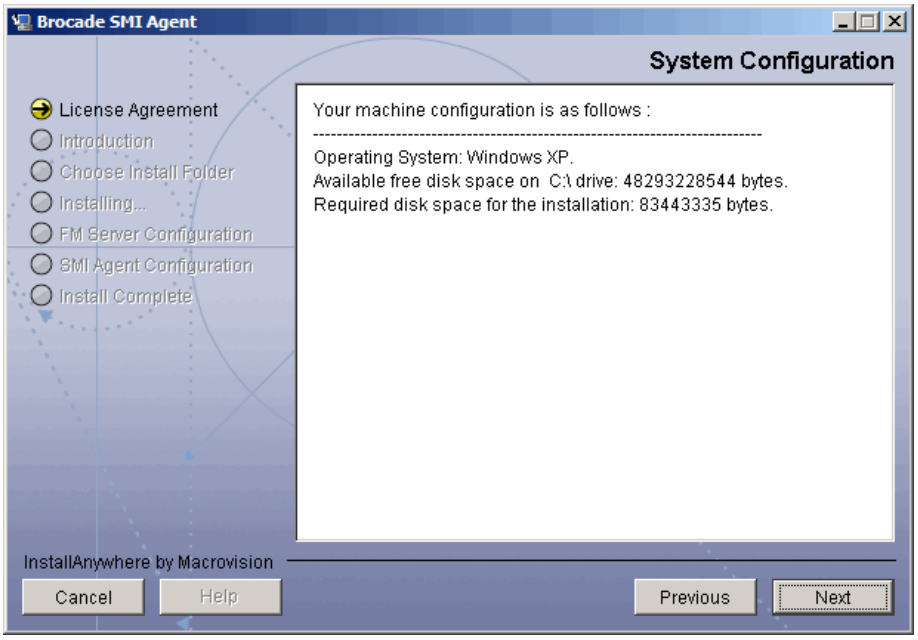


Figure 2-2 System Configuration

4. Ensure that you have the required disk space for the installation, and click **Next**.

   The Introduction window appears.

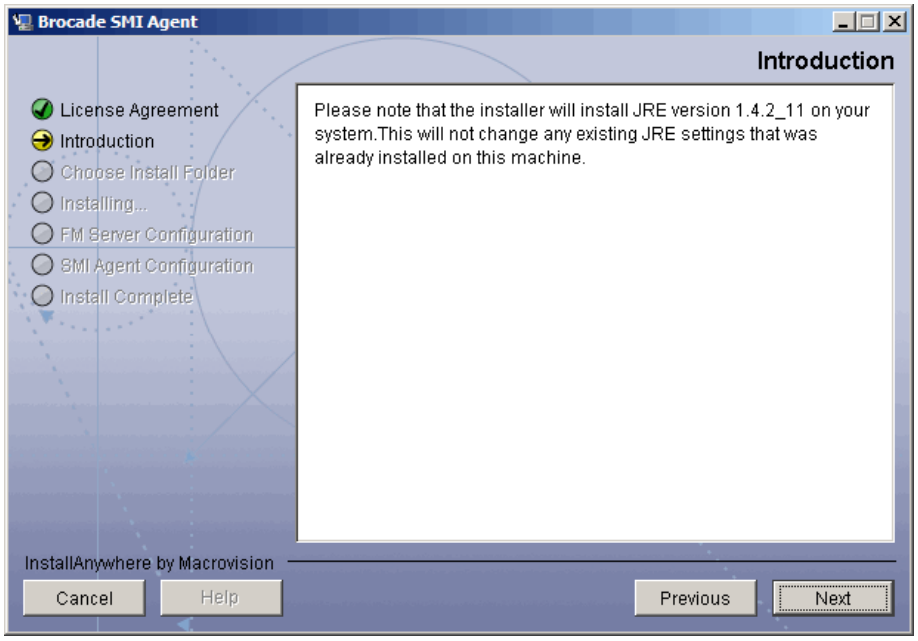


Figure 2-3 Introduction

5. Read the introduction and click **Next**.

The Choose Installation Folder window appears. The following figure shows the default installation folder for Windows, *C:\SMIAgent*.

Note

Do not specify spaces in the path or folder name.

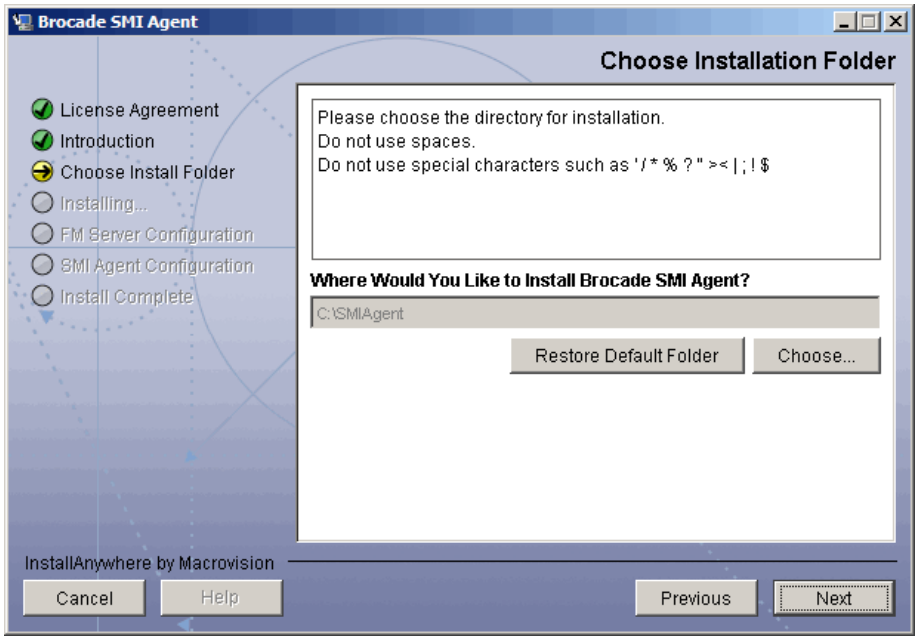


Figure 2-4 Choose Installation Folder

6. Click **Next** to accept the default installation location, or enter a different location and click **Next**.

The HTTP Port Configuration window appears. This window displays the default port number for non-secured CIMOM communication.

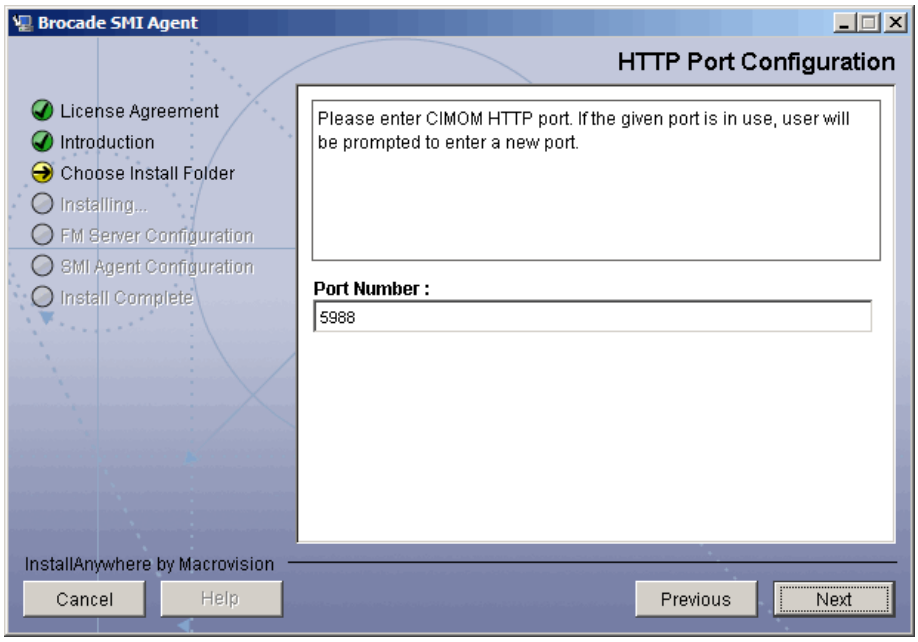


Figure 2-5 HTTP Port Configuration

7. Click **Next** to accept the default port number, or enter a new port number and click **Next**.

   If the port is in use, you get an error message and are prompted to enter a new port.

   If the port is not in use, the HTTPS Port Configuration window appears. This window displays the number that will be used for secured CIMOM communication.

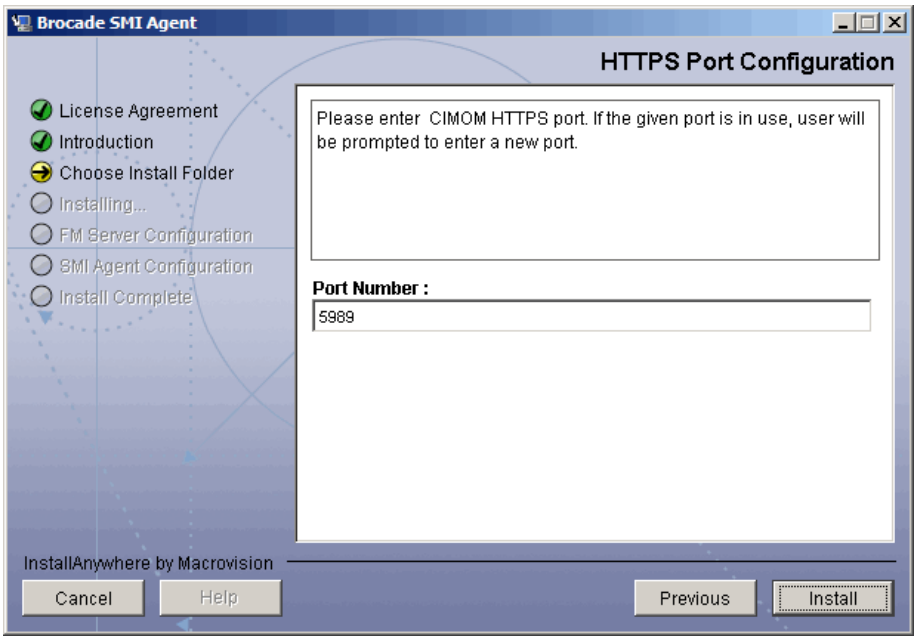


Figure 2-6 HTTPS Port Configuration

8. Click **Install** to accept the default HTTPS port number, or enter a new port number and click **Install**.

   After the installation is complete, the Fabric Manager Server Configuration window appears.

   This screen allows you to specify the connection information for an existing Brocade Fabric Manager server. Not all users have a Fabric Manager server installed and running in their environment. The information entered on this screen allows the SMI-A to report on historical port statistics by retrieving the data from the Fabric Manager database server. If your management application does not make use of historical port statistics, you do not need to enter any connection information on this screen.

   Driver This 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.

   URL The database URL should be in the form:

   ```
   jdbc:subprotocol:subname:host:port/dbname
   ```

   For example, if the Fabric Manager database 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 database servers host IP address.

   User Name The database user on whose behalf the connection is being made. The default DSN user name is: **dba**

   Password The user's password. The default DSN password is: **sql**

   This information is stored in the configuration file *SMIAgentConfig.xml* located at *<SMIAgent>\agent\server\jserver\bin*. You can use the SMI Agent Configuration tool to change these settings after installation.

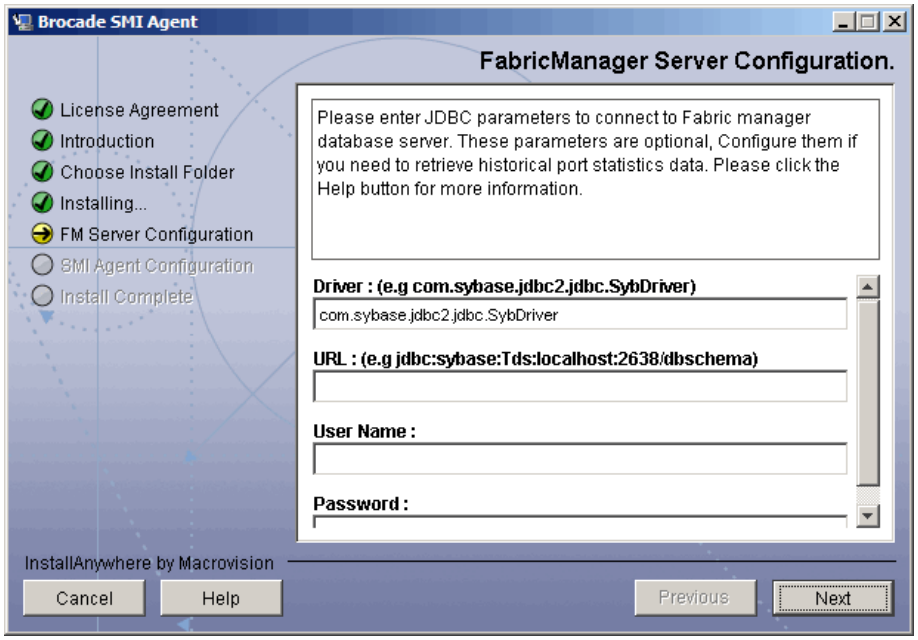


Figure 2-7 Fabric Manager Server Configuration

9. Enter database schema information, and then Click **Next**.

The Enabling Mutual Authentication for Client window appears.

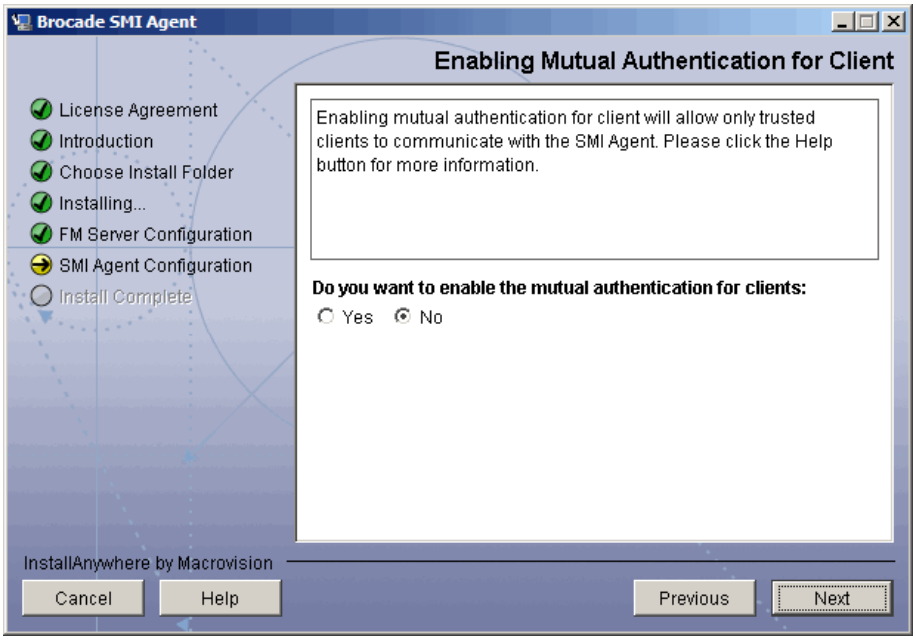


Figure 2-8 Enabling Mutual Authentication for Client

10. Choose whether to enable mutual authentication (trust by certificate) between client management applications and the Brocade SMI Agent by selecting one of the following options, and then click **Next**:

    - **Yes**: Enables mutual authentication.

      Only allow management applications that have the Brocade-provided security certificate to connect to the SMI Agent. Requires that the Brocade-provide security certificate (`server.cer`) is imported in to the truststore of the management application before a connection is established. The management application must have a mechanism that provides the client certificate (`client.cer`) during the initial handshake.

    - **No**: (Default) No mutual authentication by certificate.

      Trust by certificate is not used; however, basic encryption and local or domain authentication can still be established by enabling security in step 12.

Note

You cannot import non-Brocade certificates to the truststore of the SMI Agent.

The Enabling Mutual Authentication for Indications window appears.

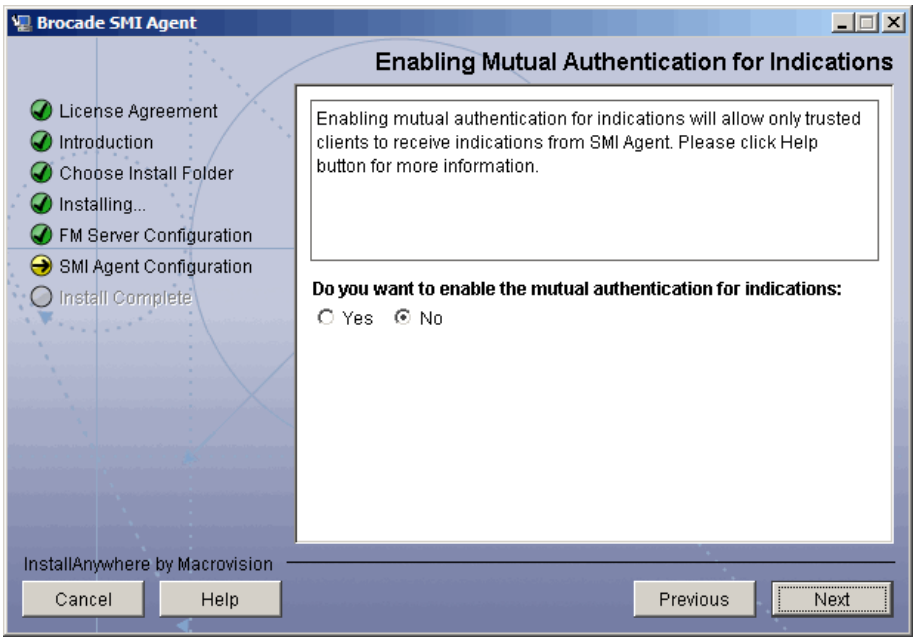


Figure 2-9 Enabling Mutual Authentication for Indications

11. Choose whether to enable mutual authentication (trust by certificate) between client management application event system and the Brocade SMI Agent by selecting one of the following options, and then click **Next**:

    - **Yes**: Enables mutual authentication.

      Only allow management applications that have the Brocade-provided security certificate to register their event system with the SMI Agent. Requires that the Brocade-provide security certificate (`serverind.cer`) is imported in to the truststore of the management application before a connection is established. The management application must have a mechanism that provides the client certificate (`clientind.cer`) during the initial handshake.

    - **No**: (Default) No mutual authentication by certificate.

      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.

Note

The SMI Agent uses this connection to send asynchronous event notifications, similar to SNMP, to the management application event system.

The Enabling Security window appears.

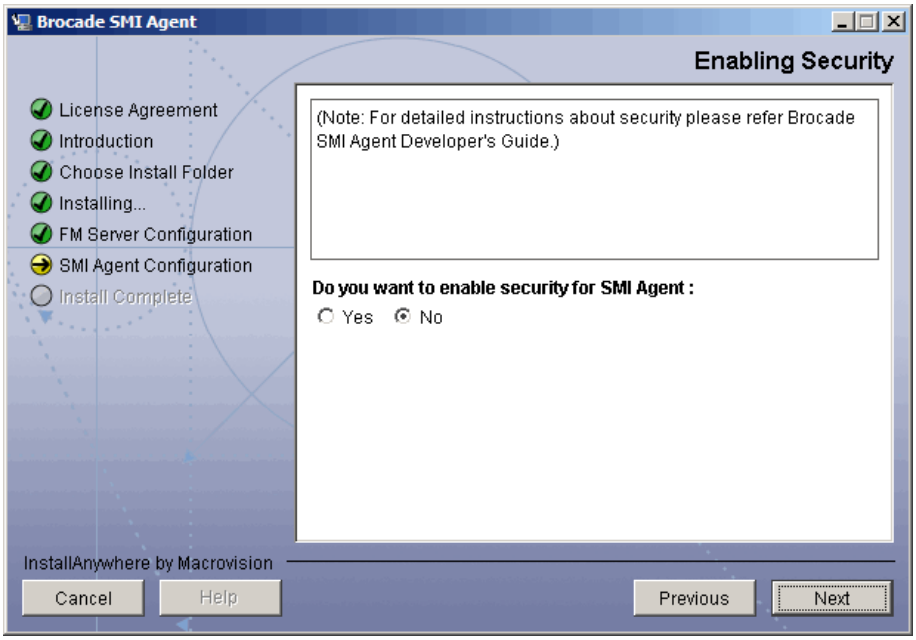


Figure 2-10 Enabling Security

12. Enable or disable authentication for SMI Agent by selecting one of the following options, and then click **Next**:

    - **Yes**: Enables authentication.

      SMI Agent validates the user name and password.

    - **No**: (Default) Disables authentication.

      SMI Agent accepts any user name and password.

One of following windows appears depending on the operating systems and setting you have selected:

- If you select No to disabled security, the Eventing and ARR TCP Port Configuration window appears, Figure 2-13, skip to step 15.
- For security enabled Solaris or Linux systems, the SMI Agent can only validate the user's credentials against the local database, the Eventing and ARR TCP Port Configuration window appears, Figure 2-13, skip to step 15.
- For security enabled Windows systems, the Enter Type of Domain Authentication window appears (shown below). Continue with the instructions in step 13 to set up user authentication for Windows.

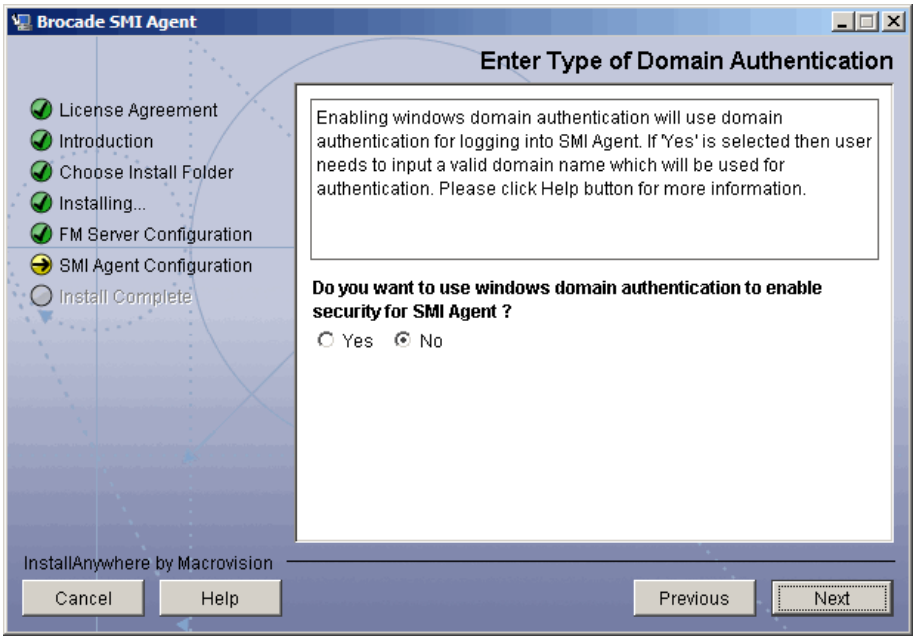


Figure 2-11 Enter Type of Domain Authentication

13. (Windows with security enabled only) Select the database you want to authenticate users as follows, and then click **Next**:

    - **Yes**: Enables domain authentication.

      SMI Agent validates the user name and password against the domain user database.

    - **No**: (Default) Disables domain authentication.

      SMI Agent validates the user against the Windows local user accounts on the SMI-A system.

One of following windows appears depending on the operating systems and setting you have selected:

- If you selected No, the Eventing and ARR TCP Port Configuration window appears; Figure 2-13, skip to step 15.
- If you selected Yes, the Enter Valid Domain Name window appears.

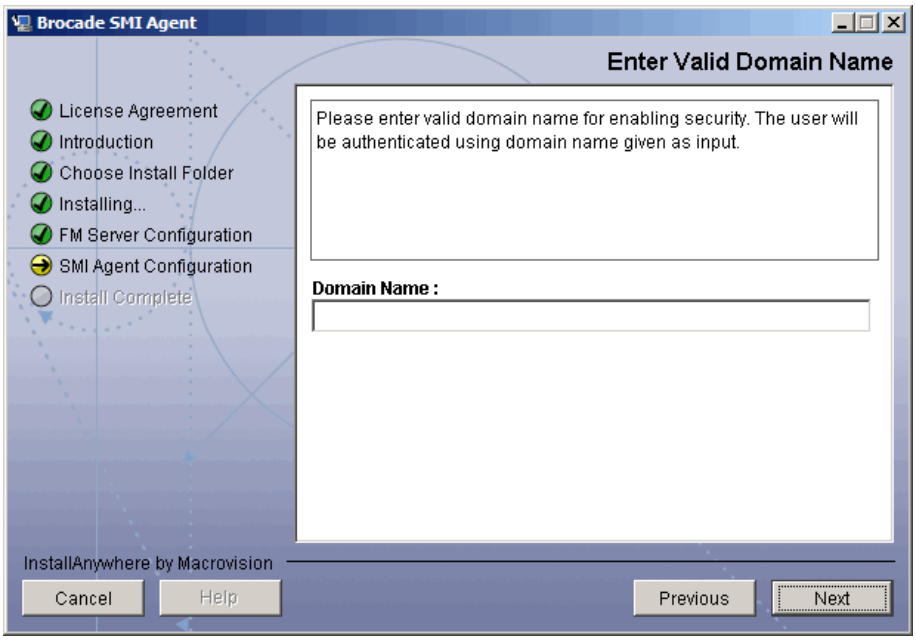


Figure 2-12 Enter Valid Domain Name

14. (Windows with domain security enabled only) Enter name of the domain which the SMI Agent will use to authenticate user credentials, and then click **Next**.

The Eventing and ARR TCP Port Configuration window appears.

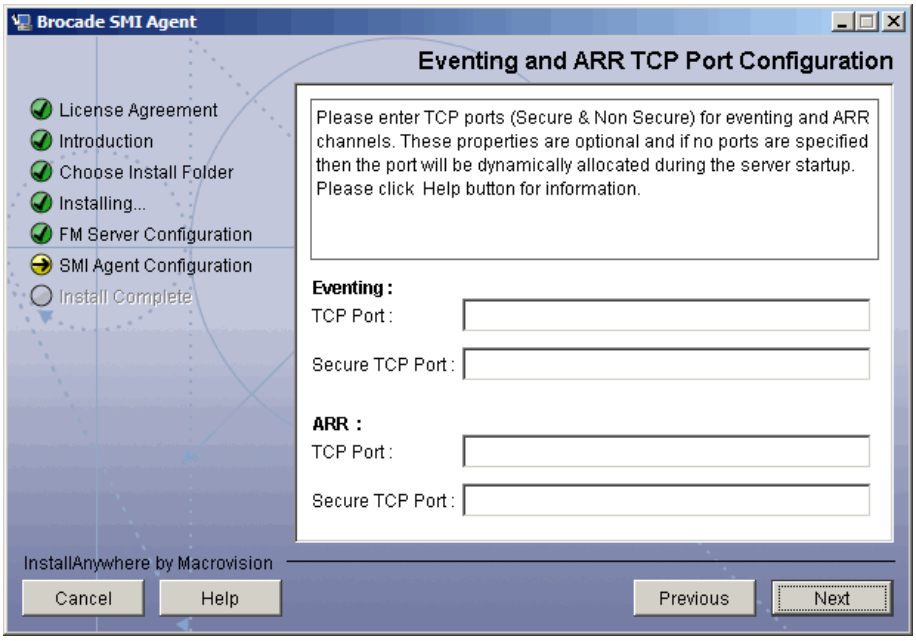


Figure 2-13 Eventing and ARR TCP Port Configuration

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.

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

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.

15. To allow the SMI Agent to allocate ports dynamically when started, enter 0 for each port number or leave this form blank, and click **Next**; to assign a specific port or range of ports, enter port numbers or range, and then click **Next**.

Note

Ports cannot be the same or in use. The SMI Agent does not verify whether or not the ports are available.

The Enabling Console And/Or File Logging window appears.

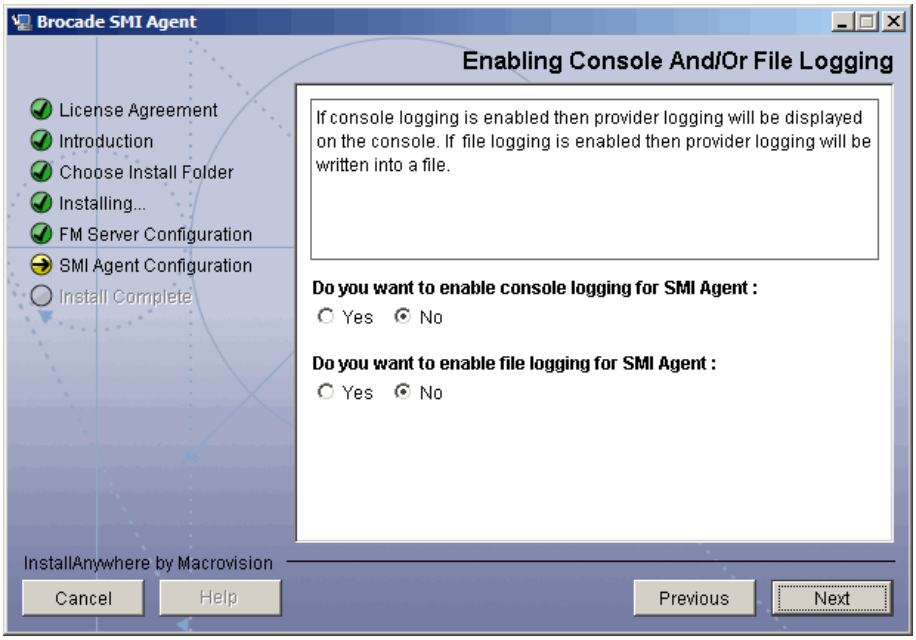


Figure 2-14 Enabling Console And/Or File Logging

16. Set up logging as follows, and then click **Next**.

    a. To display detailed messages in the console, select **Yes**.

Note

To view console messages the SMI Agent must be running from a console session, not as a service. Selecting yes to enable console messages when SMI Agent is running as a service does not affect the system.

    b. To write messages to a log file, select **Yes**.

If you enabled logging to a file the Configure Log File window appears. The following figure shows the Windows default log file name and location.

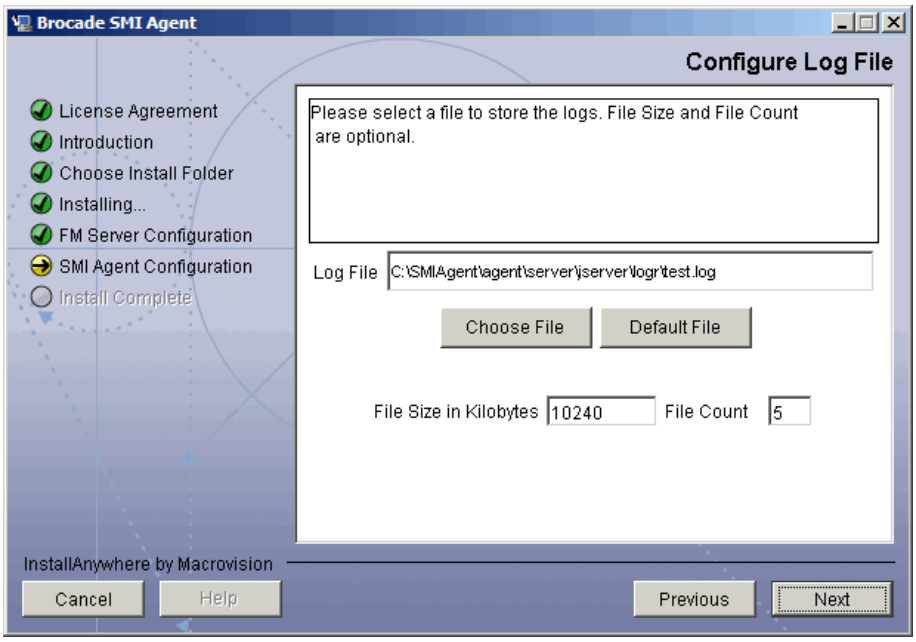


Figure 2-15 Configure Log File

c. Enter the complete path to the log file.

d. Enter the number of log files and the maximum size of the log files.

   The minimum log file size is 1 KB. The file count is a value between 1 and 10. The default is 5 log files of 10240 kilobytes (10 MB) each.

   When the specified size is exceeded on the first log file, logs will be written to the next log file.

e. Click **Next**.

   The Proxy Connections Configuration window appears.

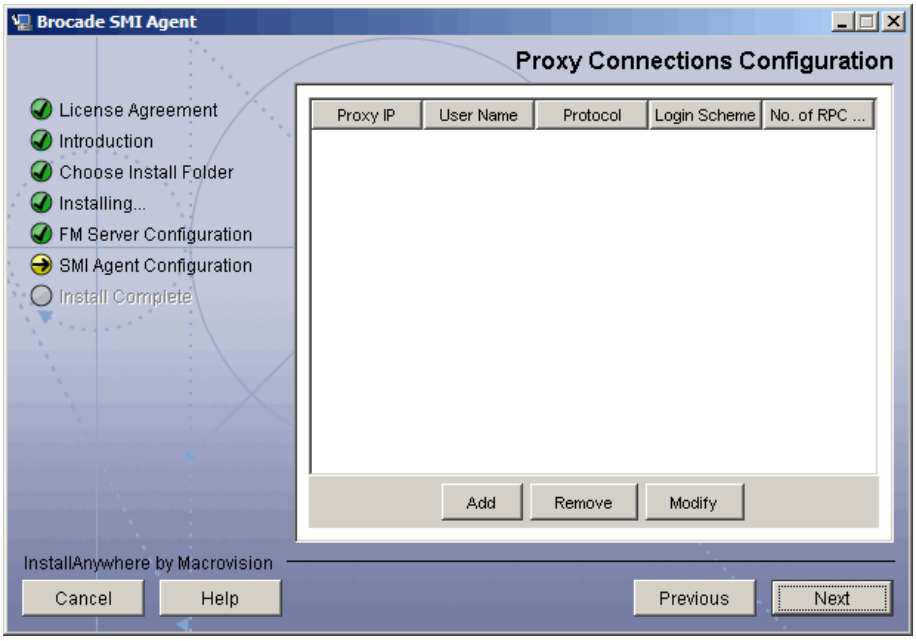


Figure 2-16 Proxy Connections Configuration

17. Configure the fabrics that you want the SMI Agent to proxy. For each fabric, click **Add** and fill out the values in the Proxy Configuration window.

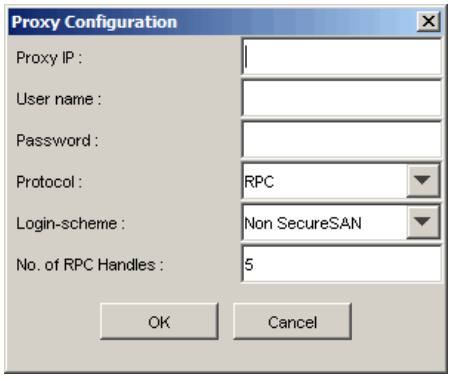


Figure 2-17 Proxy Configuration

Proxy switch IP IP address of the proxy switch (for example: 100.200.100.200)

User name Username to be used to log in to the switch (for example: admin)

Password Password to be used to log into the switch (for example: password)

Protocol Protocol: **RPC**, **Secure RPC**, or **Any**. RPC is used for a non-secure connection and Secure RPC is used for a secure connection. Any means that first a secure channel is tried and if it fails, then a non-secure channel is tried.

Login-scheme Type of login: **Non SecureSAN**, **SecureSAN**, or **Any**. Non SecureSAN is used to connect to non-secure fabrics and SecureSAN is used to connect to secure fabrics. **Any** means that SMI-A first attempts a secure connection and if it fails, attempts to connect in non-secure mode.

No. of RPC Handles Number of RPC connections to be used to connect to the switch. The possible range of values is 1 to 20. The default value is 5.

Note

Fabric OS limits the number of RPC handles allowed per switch; therefore increasing the RPC handles decreases the number of connections per switch.

18. After all the fabrics are configured in the Proxy Connections Configuration window, click **Next**.

    The Important Information window appears.

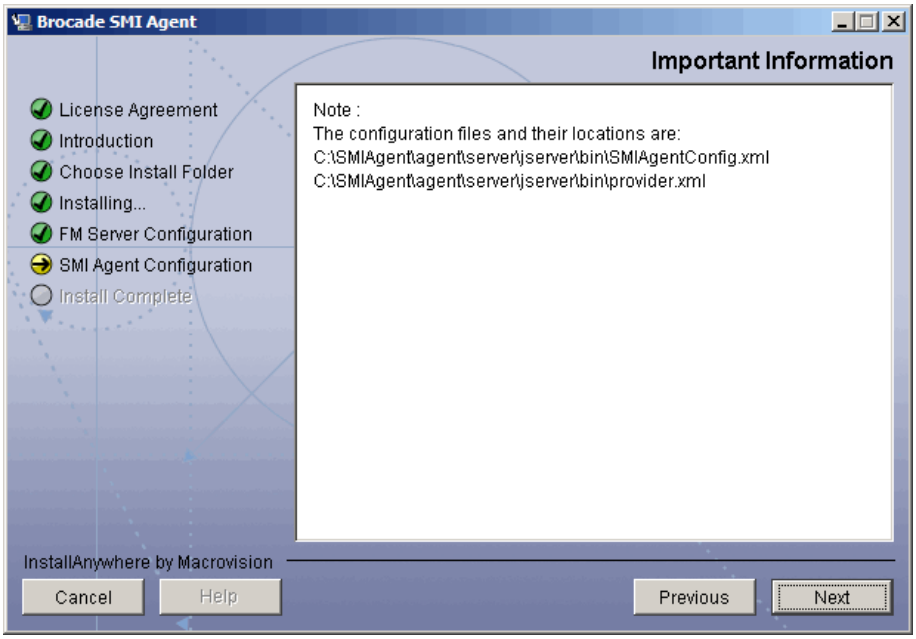


Figure 2-18 Important Information

19. Click **Next**.

The Start SMI Agent as a Windows Service window or Start Agent as a Daemon window appears.

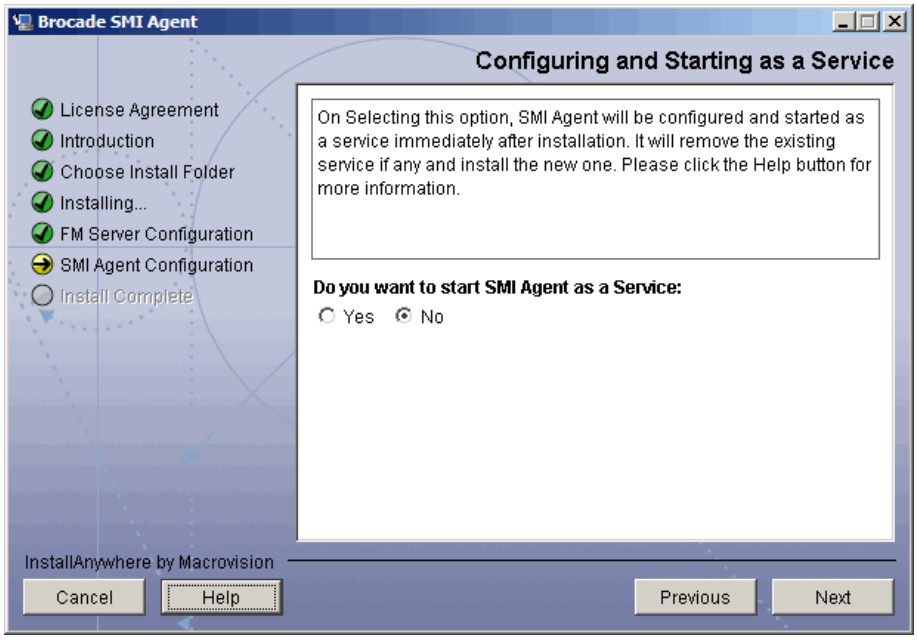


Figure 2-19 Configuring and Starting as a Service

20. Select **Yes** to start the SMI Agent as a service, and then click **Next**.

Note

If you choose not to run the SMI Agent as a service, the agent does not stop or restart automatically. You must manually start and stop the SMI Agent using the start_server script.

The Installation Completed window appears.

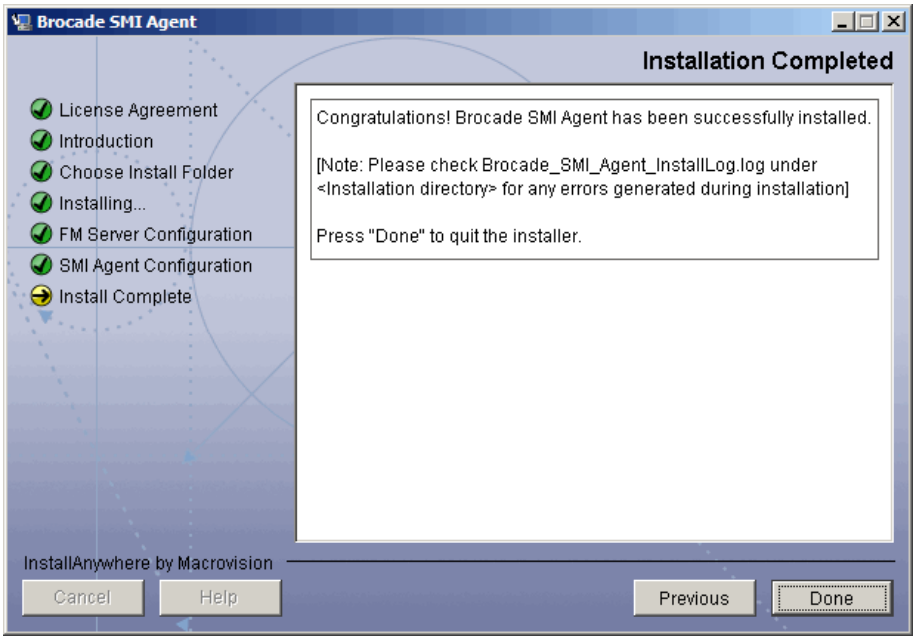


Figure 2-20 Installation Completed

21. Click **Done**.

Installing the Brocade SMI Agent in Silent Mode

You can install the SMI-A in *silent mode*, with no user intervention. In silent mode you are not prompted to enter input; instead, the installer reads input from a properties file. You are not notified of invalid inputs; however, error messages are written to a log file (the location of which is specified in the properties file).

For Windows, silent mode installation displays a splash screen while the installer is loading. This is a limitation of the InstallAnywhere installer.

Note

In silent mode, the terms of the end user license agreement cannot be displayed for acceptance. Silent installation means that, by default, you accept the same license agreement displayed during normal installation.

Creating a Properties File for Silent Installation

Prior to installation in silent mode, you must create a properties file that includes all of the properties required for agent startup. The installer will use this file to get the installation parameter values.

Brocade provides a sample properties file that you can modify:

CD_image\SilentInstallation.properties

This file contains the installation parameters listed in Table 2-1 and also contains instructions for modifying these parameters. You are required to specify values for the installation directory and the installer log file. The remaining parameters are either optional or have default values.

During silent installation, you cannot add fabric proxy information to the properties file. Configuration of proxies must be explicitly done via the *provider.xml* file or through the **LoginAsUser** extrinsic method. Refer to the *Brocade SMI Agent Developer's Guide* for more information.

Table 2-1 Installation Parameters in the SilentInstallation.properties File

OS	Parameters	Description
All	`INSTALLER_UI = silent`	The default is **silent**.
All	`USER_INSTALL_DIR =`	Required. Specify the installation directory. Spaces are not allowed in the pathname. Replace all backslashes (\) in the pathname with a double backslashes (\\). For example: `USER_INSTALL_DIR = C:\\SMIAgent`
All	`INSTALLER_LOG_FILE =`	Required. Specify the log file to which all installation messages will be written. Spaces are not allowed in the pathname. Replace all backslashes (\) in the pathname with a double backslashes (\\). For example: `INSTALLER_LOG_FILE = C:\\SMIAgent\\Install.log`
All	`CIMOM_HTTP_PORT = 5988` `CIMOM_HTTPS_PORT = 5989`	CIMOM ports (HTTP and HTTPS). Defaults are 5988 and 5989, respectively.

All	`FM_SERVER_DRIVER_INFO =`
	`FM_SERVER_URL_INFO =`
	`FM_SERVER_USER_NAME =`
	`FM_SERVER_PASSWORD =`
		Fabric Manager Server configuration information. If Fabric Manager server configuration is not required, then you do not need to specify these parameters. There are no defaults.
		See page 2-7 for more information.

All	`CLIENT_AUTH_DISABLED = 1`	Mutual authentication for clients. Default is disabled (`CLIENT_AUTH_DISABLED = 1`). To enable mutual authentication for clients, change this parameter to: `CLIENT_AUTH_ENABLED = 1` See page 2-8 for more information.
All	`IND_AUTH_DISABLED = 1`	Mutual authentication for indications. Default is disabled (`IND_AUTH_DISABLED = 1`). To enable mutual authentication for indications, change this parameter to: `IND_AUTH_ENABLED = 1` See page 2-9 for more information.

Table 2-1 Installation Parameters in the SilentInstallation.properties File (Continued)

OS	Parameters	Description
All	SECURITY_DISABLED = 1	SMI-A security. Default is disabled (SECURITY_DISABLED = 1). To enable security, change this parameter to: SECURITY_ENABLED = 1 See page 2-10 for more information.
Windows only	WINDOWS_DOMAIN_AUTH_DISABLED = 1	Windows domain authentication. This parameter is used only if security is enabled. Default is disabled (WINDOWS_DOMAIN_AUTH_DISABLED = 1). To enable Windows domain authentication, change this parameter to: WINDOWS_DOMAIN_AUTH_ENABLED = 1 See page 2-11 for more information.
Windows only	WINDOWS_DOMAIN_NAME =	Windows domain name. This parameter is required if Windows domain authentication is enabled.
All	EVENTING_PORT =	Eventing port. If not specified, or if the specified port is in use, then the port is dynamically selected at startup. See page 2-13 for more information.
All	ARR_PORT =	ARR port. If not specified, or if the specified port is in use, then the port is dynamically selected at startup. See page 2-13 for more information.
All	SECURE_EVENTING_PORT =	Secure eventing port. If not specified, or if the specified port is in use, then the port is dynamically selected at startup. See page 2-13 for more information.
All	SECURE_ARR_PORT =	Secure ARR port. If not specified, or if the specified port is in use, then the port is dynamically selected at startup. See page 2-13 for more information.
All	CONSOLE_LOGGING_DISABLED = 1	Console logging. Default is disabled (CONSOLE_LOGGING_DISABLED = 1). To enable console logging, change this parameter to: CONSOLE_LOGGING_ENABLED = 1
All	FILE_LOGGING_DISABLED = 1	File logging. Default is disabled (FILE_LOGGING_DISABLED = 1). To enable file logging, change this parameter to: FILE_LOGGING_ENABLED = 1

Table 2-1 Installation Parameters in the SilentInstallation.properties File (Continued)

OS	Parameters	Description
All	LOG_FILE_NAME =	This parameter is required only if file logging is enabled. Specify the location of the log file. Spaces are not allowed in the pathname. Replace all backslashes (\) in the pathname with a double backslashes (\\). For example: LOG_FILE_NAME = C:\\SMIAgent\\SMIAgent.log
All	LOG_FILE_COUNT = 5 LOG_FILE_SIZE = 10240	These parameters are used only if file logging is enabled. Specify the number of log files and the size of the log files. Default is 5 log files of 10240 kilobytes (10 MB) each.
All	SERVICE_DISABLED = 1	Start the SMI-A as a service. Default is no (SERVICE_DISABLED = 1). To start the SMI-A as a service, change this parameter to: SERVICE_ENABLED = 1

Triggering Silent Mode Installation

Silent mode is automatically triggered by the presence of a file named *installer.properties* in the same folder as *install.exe*. If your properties file has a different name than *installer.properties*, then you must explicitly trigger silent mode by using the **-f** option when you run the installation file.

Before starting the installation, you must ensure that the installer log file folder exists. This is the folder specified in the INSTALLER_LOG_FILE parameter.

To install the SMI-A in silent mode

1. Edit the *SilentInstallation.properties* file as described in "Creating a Properties File for Silent Installation" on page 2-19.
2. Save the properties file in the same folder as the installer executable:

   On Windows: *CD_Image\Windows*

   On Linux: *CD_Image/Linux*

   On Solaris: *CD_Image/Solaris*

   If you save the file with the name *installer.properties*, then silent mode installation is triggered automatically when you run the installation file; otherwise you must explicitly trigger silent mode installation using the **-f** option.
3. Run the installation file:

   On Windows: **CD_Image\Windows\install.exe -f "***filename***"**

   On Linux: **CD_Image/Linux/install.bin -f "***filename***"**

   On Solaris: **CD_Image/Solaris/install.bin -f "***filename***"**

   where *filename* is the name of the properties file.

If the properties file name is the default name, i*nstaller.properties*, then you can run the installation file as follows:

On Windows: **CD_Image\Windows\install.exe**

On Linux: **CD_Image/Linux/install.bin**

On Solaris: **CD_Image/Solaris/install.bin**

The SMI-A is installed to the location specified in the `USER_INSTALL_DIR` parameter of the properties file.

The status of the installation, along with any error messages, is reported in the installation log file, which is in the location specified in the `INSTALLER_LOG_FILE` parameter of the properties file. The status of the installation is SUCCESS only if all of the installation operations succeeded; otherwise, the overall installation status is FAILED. Refer to Chapter 3, “Silent Installation Status Messages” for details about the status messages.

Post-Installation Considerations

The Brocade SMI Agent supports SLP to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks. If you want Service Location Protocol (SLP) support, you must install and start the SLP daemon prior to starting the SMI-A. See the *Brocade SMI Agent User’s Guide* for instructions on installing and starting the SLP daemon.

After you install the SMI-A, you can change many of the configuration settings using the Brocade SMI Agent Configuration Tool. For example, you can:

- reconfigure the ports used by the SMI-A
- enable and disable logging and configure different levels of logging
- add and remove fabrics

See the *Brocade SMI Agent User’s Guide* for instructions on using this tool.

Uninstalling the Brocade SMI Agent

The uninstaller automatically uninstalls the SMI-A in the same way you installed it: either using the wizard or in silent mode.

The JRE that was installed when you installed the SMI-A is removed as part of the uninstallation.

To uninstall the SMI-A

1. Click the “Uninstall Brocade SMI Agent” shortcut on the **Start** menu.

   or

   Type the following at the command line:

   On Windows: `<SMIAgent>\UninstallerData\"Uninstall Brocade SMI Agent.exe"`

   On Linux or Solaris: `./<SMIAgent>/UninstallerData/Uninstall_Brocade_SMI_Agent`

If you installed the SMI-A using the wizard, the Uninstall wizard launches and directs you through the uninstallation process (see Figure 2-21).

If you installed the SMI-A in silent mode, the SMI-A is automatically uninstalled in silent mode.

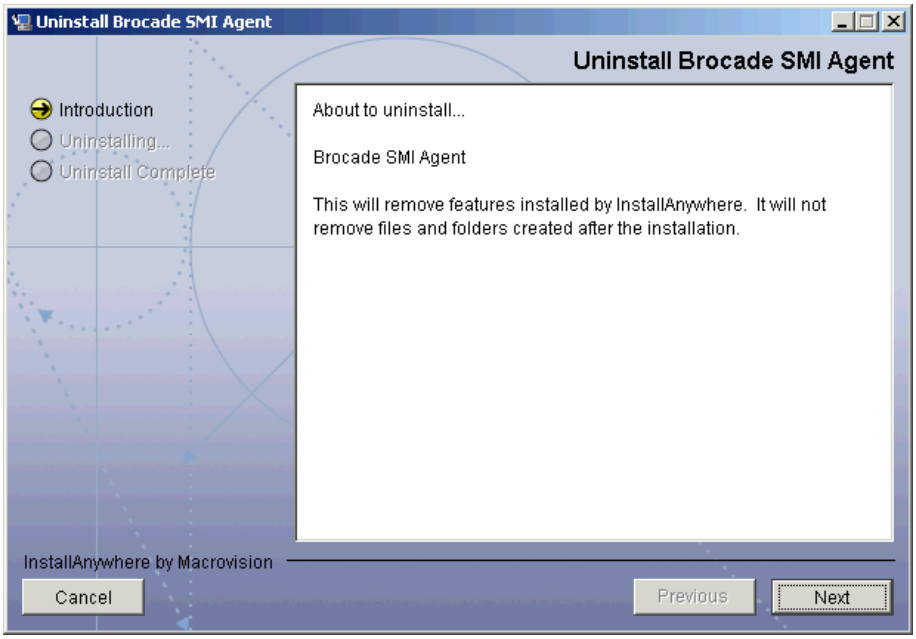


Figure 2-21 Uninstalling the Brocade SMI Agent

Silent Installation Status Messages

Chapter 3

When you install the SMI-A in silent mode, status messages are written to the installation log file, the name and location of which is specified in the properties file.

The format of each status message is:

```
SMIAgent;1.0.0;Operation=opname;Status=status;StatusCode=code;StatusMessage=msg;
```

where *opname* is the name of the operation, *status* is either Passed or Failed, *code* is the numeric status code, and *msg* is the status message.

Table 3-1 lists the possible operation names and, for each operation, the possible status, status codes, and status messages.

Table 3-1 Silent Installation Error Codes

Operation Name	Status	Status Code	Status Message
Choose Installer Folder Name	Passed	0	Successful
	Failed	-1	Your system drive does not have disk space required for the installation
	Failed	-2	Invalid Folder
	Failed	-3	Installation Folder Name contains a space
CIMOM Ports Configuration	Passed	0	CIMOM Ports Configured
	Failed	-5	Configured HTTP port in use
	Failed	-5	Configured HTTPS port in use
	Failed	-6	Invalid Port Range
	Failed	-7	Non Numeric or Negative CIMOM Ports
	Failed	-16	HTTP and HTTPS cannot be the same
FM Server Configuration	Passed	0	Successful
Mutual Authentication for Client	Passed	0	Disabled Mutual Authentication for SMI Agent
	Passed	0	Enabled Mutual Authentication for SMI Agent
	Failed	-5	Configured HTTP port in use
	Failed	-22	Invalid Parameter for Mutual Authentication for Client

Table 3-1 Silent Installation Error Codes

Operation Name	Status	Status Code	Status Message
Mutual Authentication for Indication	Passed	0	Disabled Mutual Authentication for Indication
	Passed	0	Enabled Mutual Authentication for Indication
	Failed	-5	Configured HTTP port is in use
	Failed	-22	Invalid Parameter for Mutual Authentication for Indication
Eventing and ARR Configuration	Passed	0	Eventing and ARR ports configured
	Failed	-6	Invalid Port Range
	Failed	-10	Ports used for Eventing and ARR cannot be the same
	Failed	-11	Eventing Port value should not be negative
	Failed	-12	ARR Port value should not be negative
	Failed	-17	Invalid or Non-numeric port
	Failed	-18	Port used for Eventing is already configured as HTTP or HTTPS port
	Failed	-19	Port used for ARR is already configured as HTTP or HTTPS port;
Secure Eventing and ARR Configuration	Passed	0	Secure Eventing and ARR ports configured
	Failed	-23	Port used for Secure ARR is already configured as HTTP or HTTPS port, or is negative
	Failed	-24	Ports used for Secure Eventing and Secure ARR cannot be the same
	Failed	-25	Ports used for Secure Eventing and Eventing cannot be the same
	Failed	-26	Ports used for Secure Eventing and ARR cannot be the same
	Failed	-27	Ports used for Secure ARR and Eventing cannot be the same
	Failed	-28	Ports used for Secure ARR and ARR cannot be the same
	Failed	-29	Invalid port number provided for Secure ARR or Eventing port. The valid port range is 0–65535.
	Failed	-30	Port used for Secure Eventing is already configured as HTTP or HTTPS port, or is negative.

Table 3-1 Silent Installation Error Codes

Operation Name	Status	Status Code	Status Message
Security	Passed	0	Disabled Security for SMI Agent.
	Passed	0	Enabled Security for SMI Agent.
	Passed	0	Enabled Security for SMI Agent without Windows domain authentication
	Failed	-5	Configured HTTP port is in use
	Failed	-8	You should be a root user to enable security
	Failed	-9	Windows domain name should not be empty for enabling security on Windows
	Failed	-20	Windows domain authentication failed
	Failed	-21	Windows domain authentication failed. Failed to stop the server.
	Failed	-22	Invalid Parameter for Security
Console Logging	Passed	0	Enabled Console Logging
	Passed	0	Disabled Console Logging
	Failed	-22	Invalid Parameter for Console Logging
File Logging	Passed	0	Disabled File Logging
	Passed	0	Enabled File Logging
	Failed	-13	Invalid Log File Size
	Failed	-14	Invalid file size count
	Failed	-15	Empty File location
	Failed	-22	Invalid Parameter for File Logging
SMI Agent as Service	Passed	0	Disabled SMI Agent as Service
	Passed	0	Enabled SMI Agent as Service
	Passed	0	Installer has detected that already one SMI Agent is installed as a service. This operation will remove the old one and install the new one
	Failed	-8	You should be a root user to install SMI Agent as a service
	Failed	-22	Invalid Parameter for SMI Agent as Service
Installation	Passed	0	SMI Agent was Successfully installed on your machine.
	Failed	-25	SMI Agent Overall Installation failed.

Frequently Asked Questions

Chapter 4

This chapter contains questions most frequently sent to the SMI Agent Developer Support email address.

- Besides Windows Domain authentication, does the SMI Agent support local user authentication?
- What are the Eventing and ARR TCP Ports? Do they relate to indications?
- What encryption method is used to encrypt the password field in provider.xml?
- How do I report a problem and what information should I provide?
- 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?
- Can the SMI Agent proxy for two fabrics that are in different subnets?
- In using Windows domain authentication, do I need to include the domain name along with the username for authentication?
- What are some situations that might require restarting the SMI Agent?
- Should I designate multiple proxies into a fabric? What are the best practices concerning this?

See the "Frequently Asked Questions" chapter in the *Brocade SMI Agent User's Guide* for additional questions and answers.

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

SMIAgent 110.4.0 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 Agent 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 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.

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 and Solaris: *<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.

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. If the switches in the fabric do not all have the same Fabric OS version, then you should designate the switch with the highest supported Fabric OS version as the proxy. It is not necessary to choose the principal switch as the proxy.

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

Yes.

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");
```

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.

How do I start and stop the SMI Agent?

See the *Brocade SMI Agent User's Guide* for instructions on starting and stopping the SMI Agent.

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.

Index

D

Distributed Management Task Force (DMTF) x

E

error codes for silent installation 3-1

F

Fibre Channel Association x
frequently asked questions (FAQs) 4-1

H

help, SMI agent support xi

I

installation requirements 1-1
installing SMI-A as a service 2-1
installing SMI-A on Windows 2-2

P

platform support 1-1

R

requirements for installation 1-1
return codes for silent installation 3-1

S

silent installation
- error codes 3-1
- on Windows 2-19

SMI-A
- installing as a service 2-1
- installing on Windows 2-2
- uninstalling 2-23

Storage Management Initiative (SMI) x
Storage Management Initiative Specification (SMI-S) x
Storage Networking Industry Association (SNIA) x
supported platforms 1-1

U

uninstalling SMI-A 2-23

W

Web Based Enterprise Management (WBEM) x