IBM® Storage Networking

IBM Network Advisor SAN Installation and Migration Guide

Supporting IBM Network Advisor version 14.4.2

NOTE
This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

GC27-6622-04

GC27-6622-04

Contents

About This Document

What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
  - None
- Information that was changed:
  - Updated release version wherever applicable.
  - Updated Installation and Migration support.
  - Updated Server and client operating system requirements.
- Information that was deleted:
  - None

For further information about new features and documentation updates for this release, refer to the IBM Network Advisor 14.4.2 release notes.

Supported hardware and software

When procedures or parts of procedures documented in this guide apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for IBM Network Advisor 14.4.2, documenting all possible configurations and scenarios is beyond the scope of this guide.

Fabric OS software support

The following firmware platforms are supported by this release of the IBM Network Advisor 14.4.2:

- Fabric OS 6.0 or later
- Fabric OS 7.0 or later
- Fabric OS 8.0 or later
- Fabric OS 8.1 or later
- Fabric OS 8.2 or later

NOTE

Discovery of a secure Fabric OS fabric in strict mode is not supported.

NOTE
To ensure that a configuration is fully supported, always check the appropriate SAN, storage or blade server product support page to verify support of specific code levels on specific switch platforms prior to installing on your switch. Use only Fabric OS versions that are supported by the provider.

Fabric OS hardware support

The hardware platforms in the following table are supported by this release of the IBM Network Advisor 14.4.2.

NOTE
Professional and Professional Plus (Trial and Licensed) versions of the IBM Network Advisor 14.4.2 can discover, but not manage 8-slot directors. These devices cannot be used as a Seed switch.

TABLE 1 Hardware supported by Fabric OS

Device name	Terminology used in documentation	Firmware level required
SAN24B-4	24-port, 8-Gbps FC switch	Fabric OS v7.0.0 or later
SAN40B-4	40-port, 8-Gbps FC switch	Fabric OS v7.0.0 or later
SAN80B-4	80-port, 8-Gbps FC switch	Fabric OS v7.0.0 or later
SAN24B-5	24-port, 16-Gbps Edge switch	Fabric OS v7.0.1 or later
SAN48B-5	48-port, 16-Gbps Gbps switch	Fabric OS v7.0.0 or later
SAN96B-5	96-port, 16 Gbps switch	Fabric OS v7.1.0 or later
SAN06B-R	8Gbps extension switch	Fabric OS v7.0.0 or later
SAN42B-R	16 Gbps 24-FC port, 18 GbE port switch	Fabric OS v7.3.0 or later
IBM Converged Switch B32	8 Gbps 8-FC-port, 10 GbE 24-CEE port switch	Fabric OS v6.1.2_CEE
SAN32B-E4 Encryption Switch	8 Gbps encryption switch	Fabric OS v6.1.1_enc or later
IBM Storage Networking SAN24B-6	24-port, 32 Gbps switch	Fabric OS v8.1.0 or later
IBM Storage Networking SAN64B-6	64-port, 32 Gbps switch	Fabric OS v8.0.0 or later
IBM Storage Networking SAN128B-6	96-port, 32 Gbps switch	Fabric OS v8.2.0 or later
SAN768B	8-port backbone chassis	Fabric OS v6.0.0 or later
SAN768B with FC8-16, FC8-32, and FC8-48 Blades	8-port backbone chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades	Fabric OS v7.0.0 or later
SAN768B with FC8-64 Blade	8-port backbone chassis with 8 Gbps 64-port blade	Fabric OS v7.0.0 or later
SAN768B with FC10-6 Blade	8-port backbone chassis with FC 10 - 6 ISL blade	Fabric OS v7.0.0 or later
SAN768B with FX8-24 Extension Blade	8-port backbone chassis with 8 Gbps extension blades	Fabric OS v6.3.1 or later
SAN768B with FCoE10-24 Blade	8-port backbone chassis with 8 Gbps 24-port FCoE blades	Fabric OS v6.3.1 or later
SAN768B with FS8-18 Blade	8-port backbone chassis with Encryption blade	Fabric OS v6.1.1_enc or later
SAN384B	4-port backbone chassis	Fabric OS v7.0.0 or later
SAN384B with FC8-16, FC8-32, and FC8-48 Blades	4-port backbone chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades	Fabric OS v7.0.0 or later
SAN384B with FC8-64 Blade	4-port backbone chassis with 8 Gbps 64-port blade	Fabric OS v7.0.0 or later

TABLE 1 Hardware supported by Fabric OS (continued)

Device name	Terminology used in documentation	Firmware level required
SAN384B with FC10-6 Blades	4-port backbone chassis with FC 10 - 6 ISL blades	Fabric OS v7.0.0 or later
SAN384B with FX8-24 Extension Blades	4-port backbone chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports extension blades	Fabric OS v7.0.0 or later
SAN384B with FCoE10-24 Blade	4-port backbone chassis with 8 Gbps 24-port FCoE blade	Fabric OS v7.0.0 or later
SAN384B with FS8-18 Blade	4-port backbone chassis with Encryption blade	Fabric OS v6.1.1_enc or later
SAN384B-2	16 Gbps 4-port backbone chassis	Fabric OS v7.0.0 or later
SAN768B-2	16 Gbps 8-port backbone chassis	Fabric OS v7.0.0 or later
IBM Storage Networking SAN256B-6	32 Gbps, 4-slot backbone chassis	Fabric OS v8.0.1 or later
IBM Storage Networking SAN512B-6	32 Gbps, 8-slot backbone chassis	Fabric OS v8.0.1 or later
FC8-16 Blade Only supported on the SAN384B and SAN768B chassis.	FC 8 GB 16-port blade	Fabric OS v7.0.0 or later
FC8-32 Blade Only supported on the SAN384B and SAN768B chassis.	FC 8 GB 32-port blade	Fabric OS v7.0.0 or later
FC8-32E Blade Only supported on the SAN384B-2 and SAN768B-2 chassis.	FC 8 GB 32-port blade	Fabric OS v7.0.1 or later
FC8-48 Blade Only supported on the SAN384B and SAN768B chassis.	FC 8 GB 48-port blade	Fabric OS v7.0.0 or later
FC8-48E Blade Only supported on the SAN384B-2 and SAN768B-2 chassis.	FC 8 GB 48-port blade	Fabric OS v7.0.1 or later
FC8-64 Blade	FC 8 GB 64-port blade	Fabric OS v7.0.0 or later
FC10-6 Blade	FC 10 - 6 ISL blade	Fabric OS v7.0.0 or later
FC16-32 Blade Only supported on the SAN384B-2 and SAN768B-2 chassis.	16 Gbps 32-port blade	Fabric OS v7.0.0 or later
FC16-48 Blade Only supported on the SAN384B-2 and SAN768B-2 chassis.	16 Gbps 48-port blade	Fabric OS v7.0.0 or later
FC16-64 Blade Only supported on the SAN384B-2 and SAN768B-2 chassis.	16 Gbps 64-port blade	Fabric OS v7.0.0 or later
FCoE10-24 Blade Only supported on the SAN768B, SAN384B, and SAN768B-2 chassis.	10 Gig FCoE port router blade	Fabric OS v7.0.0 or later
FX8-24 Extension Blade	8 Gbps extension blade	Fabric OS v6.3.1_CEE
FC32-48 Port Blade	32 Gbps 48-port blade	Fabric OS v8.0.1 or later

TABLE 1 Hardware supported by Fabric OS (continued)

Device name	Terminology used in documentation	Firmware level required
FC32-64 Port Blade	32 Gbps 64-port blade	Fabric OS v8.2.0 or later
SX6 Extension Blade	32 Gbps, router extension blade	Fabric OS v8.0.1 or later

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
	In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].

Convention	Description
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the 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 a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Getting technical help

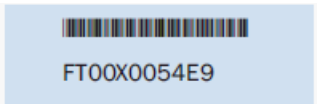
Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

- Management application serial number

To obtain the Management application serial number, select **Help > License**. The **License** dialog box displays.

- 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
  - Logs from serial console and Telnet sessions
  - Logs from syslog messages
- 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:

- SAN24B-4, SAN24B-5, SAN24B-6, SAN42B-R, SAN64B-6, SAN40B-4, SAN80B-4, SAN96B-5, SAN06B-R, and IBM Converged Switch B32—On the switch ID pull-out tab located inside the chassis on the port side on the left
- SAN48B-5—On the pull-out tab on the front of the switch
- SAN256B—Inside the chassis next to the power supply bays
- SAN768B and SAN768B-2—On the bottom right on the port side of the chassis
- SAN384B and SAN384B-2—On the bottom left on the port side of the chassis
- SAN256B-6 and SAN512B-6—On the upper portion of the chassis to the left of the fan assemblies

- World wide name (WWN)

You can also obtain the WWN from the same place as the serial number. For the SAN768B, SAN384B, SAN768B-2, SAN256B-6, and SAN512B-6, access the numbers on the WWN cards by removing the WWN bezel at the top of the nonport side of the chassis. If the switch is operable, you can also use the **wwn** command to display the switch WWN.

How to send your comments

Your feedback is important in helping us provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, send us your comments by e-mail to starpubs@us.ibm.com.

Be sure to include the following:

- Exact publication title (paste into the e-mail subject line)
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Installation

System requirements

Use the following sections to determine if you have met the requirements for the Management application.

- Server and client operating system requirements on page 11
- Memory, host, and disk space requirements
- Operating system cache requirements on page 16
- Browser requirements on page 17
- Client and server system requirements on page 17

Server and client operating system requirements

Table 2 summarizes the required operating systems for servers and the packages supported by each OS version.

NOTE
It is recommended that you run Management application on a dedicated machine to avoid conflicts with other applications that use the same resources and ports (such as SNMP, a web server, and so on).

NOTE
Beginning with version 14.0.0, the 32-bit installer is not supported.

NOTE
If the required operating system is not available, a warning message displays during installation.

TABLE 2 Server operating system requirements

Operating system	Version	Guest OS version	Supported packages
Windows®	• Windows Server 2008 R2 SP1 Datacenter Edition (x86 64-bit) • Windows Server 2008 R2 SP1 Standard Edition		SAN with SMI Agent SMI Agent only

TABLE 2 Server operating system requirements (continued)

Operating system	Version	Guest OS version	Supported packages
	(x86 64-bit) • Windows Server 2008 R2 SP1 Enterprise Edition (x86 64-bit) • Windows Server 2012 R2 Datacenter Edition (x86 64-bit) • Windows Server 2012 R2 Standard Edition (x86 64-bit) • Windows Server 2016 Datacenter Edition (x86 64-bit) • Windows Server 2016 Standard Edition (x86 64-bit) • Windows 10 Enterprise (x86 64-bit)		
Linux®	• Red Hat Enterprise Linux 6.8 Advanced (x86 64-bit) • Red Hat Enterprise Linux 6.9 Advanced (x86 64-bit)		SAN with SMI Agent SMI Agent only

TABLE 2 Server operating system requirements (continued)

Operating system	Version	Guest OS version	Supported packages
	• Red Hat Enterprise Linux 7.1 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.2 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.3 Advanced (x86 64-bit) • SuSE Linux Enterprise Server 11.3 (x86 64-bit) • SuSE Linux Enterprise Server 12 (x86 64-bit) • Oracle Enterprise Linux 6.8 (x86 64-bit) • Oracle Enterprise Linux 6.9 (x86 64-bit) • Oracle Enterprise Linux 7.1 (x86 64-bit) • Oracle Enterprise Linux 7.2 (x86 64-bit) • Oracle Enterprise Linux		

TABLE 2 Server operating system requirements (continued)

Operating system	Version	Guest OS version	Supported packages
	7.3 (x86 64-bit)		
Guest VMs	• VMware® ESXi 6.0 • VMware® ESXi 6.5 • Microsoft Hyper-V (Hyper-V Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Datacenter, and Windows Server 2016) • KVM RH 6.8 • KVM RH 7.0 • KVM RH 7.1 • KVM RH 7.2	Supports all server OS versions available for Windows and Linux.	Supports all packages available for Windows and Linux.

Table 3 summarizes the required OS for clients. Management application clients are supported on 64-bit Windows and Linux systems.

TABLE 3 Client operating system requirements

Operating system	Version	Guest OS version
Windows®	• Windows Server 2008 R2 SP1 Datacenter Edition (x86 64-bit) • Windows Server 2008 R2 SP1 Standard Edition (x86 64-bit) • Windows Server 2008 R2 SP1 Enterprise Edition (x86 64-bit) • Windows Server 2012 R2 Datacenter Edition (x86 64-bit) • Windows Server 2012 R2 Standard Edition (x86 64-bit) • Windows Server 2016 Datacenter Edition (x86 64-bit)	

TABLE 3 Client operating system requirements (continued)

Operating system	Version	Guest OS version
	• Windows Server 2016 Standard Edition (x86 64-bit) • Windows 7 Enterprise (x86 64-bit) • Windows 8.1 Enterprise (x86 64-bit) • Windows 10 Enterprise (x86 64-bit)	
Linux®	• Red Hat Enterprise Linux 6.8 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.0 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.1 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.2 Advanced (x86 64-bit) • Red Hat Enterprise Linux 7.3 Advanced (x86 64-bit) • SuSE Linux Enterprise Server 11.3 (x86 64-bit) • SuSE Linux Enterprise Server 12 (x86 64-bit) • Oracle Enterprise Linux 7.0 (x86 64-bit) • Oracle Enterprise Linux 7.1 (x86 64-bit) • Oracle Enterprise Linux 7.2 (x86 64-bit) • Oracle Enterprise Linux 7.3 (x86 64-bit)	
Guest VMs	• VMware® ESXi 5.5 • VMware® ESXi 6.0 • Microsoft Hyper-V (Hyper-V Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Data Center, Windows Server 2016) • KVM RH 6.8 • KVM RH 7.0 • KVM RH 7.1 • KVM RH 7.2	Supports all client OS versions available for Windows and Linux.

Memory, host, and disk space requirements

Memory requirements are applicable only when there are no other applications running on the Management application server. Paging space should be equal to or exceed the physical memory size.

NOTE

You must allocate 2 GB of client memory and 6 GB of server memory to efficiently manage more than 9,000 SAN ports. It is not recommended to allocate more than 6 GB of server memory.

NOTE
If you use sFlow, it is recommended that you add an additional 100 GB of disk space.

NOTE
It is recommended that you add an additional 40 GB of disk space for the default temporary directory.

NOTE
If you enable periodic supportSave or configure the Management application server as the Upload Failure Data Capture location for monitored switches, you must add additional disk space. Each switch supportSave file is approximately 5 MB, and each Upload Failure Data Capture file is approximately 500 KB. To determine the disk space requirements, multiply the frequency of scheduled supportSave files by 5 MB and the expected Upload Failure Data Capture files by 500 KB before the planned periodic purge activity.

The following table summarizes the memory, host, and disk space requirements for a remote client.

TABLE 4 Memory, host, and disk space requirements for remote client

Resources	Small	Medium	Large
Installed memory	4 GB	4 GB	8 GB
Processor core count (including physical and logical cores)	2 (1 physical, 2 virtual)	4 (2 physical, 4 virtual)	8 (4 physical, 8 virtual)
Disk space	1 GB	1 GB	1 GB

The following table summarizes the minimum system requirements for server (plus 1 client) installation.

TABLE 5 Minimum system requirements for server (plus 1 client) installation

Resources	Professional edition	Professional Plus or Enterprise edition Enterprise edition
Installed memory	6 GB	6 GB
Processor core count (including physical and logical cores)	2	2
Disk space	10 GB	20 GB

The following table summarizes the recommended system requirements for server (plus 1 client) installation.

TABLE 6 Recommended system requirements for server (plus 1 client) installation

Resources	Small	Medium	Large
Installed memory	16 GB	16 GB	16 GB
Processor core count (including physical and logical cores)	2 (1 physical, 2 virtual)	4 (2 physical, 4 virtual)	8 (4 physical, 8 virtual)
Disk space	20 GB	80 GB	100 GB

Operating system cache requirements

It is recommended that you use the system-managed size (the OS allocates the required cache); however, if you choose to use a custom size, make sure you that use the following memory settings for your operating system.

The virtual memory requirement for Windows systems is 1 GB for minimum paging file size and 4 GB for maximum paging file size.

NOTE
For networks with more than 9,000 ports, the recommended memory allocation is 6 GB.

TABLE 7 Linux swap space requirements

Installed physical memory (RAM) size	Recommended swap size
Greater than 4 GB and less than 8 GB	Equal to the amount of RAM
Greater than or equal to 8 GB and less than 64 GB	5 times the amount of RAM

Browser requirements

The launch of Management application remote client and the launch of the Server Management Console, Launch in Context (LIC), and the Element Manager (Web Tools) from the application are supported by the following browsers with a Java plug-in:

The launch of Management application remote client, and the launch of the Server Management Console and Launch in Context (LIC) from the application are supported from the following browsers with a Java plug-in:

- Browsers
  - Windows Internet Explorer 11.0.9 on Windows (except Windows 8 and 2012)
  - Firefox 54 or later on Windows
  - Google Chrome 59 on Windows
  - Edge 40 on Windows 10
- Java Plug-ins: For the current supported JRE version for the Management application remote client, and the launch of the Server Management Console, Launch in Context (LIC), and Web Tools, refer to the release notes.

  NOTE
  For higher performance, use a 64-bit JRE.

  NOTE
  If the minimum system requirement is not met, you will be blocked from the configuration, and an error message will be displayed.

For the website listing patch information, go to http://www.oracle.com/technetwork/java/javase/downloads/index.html.

Launching Management application in the IE and Edge browsers

You can launch Management application in Internet Explorer 10 or later and in Edge browsers using a literal IPv6 address.

We recommend the *xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx.ipv6-literal.net* literal IPv6 address format instead using the standard [xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] IPv6 format.

Client and server system requirements

NOTE
Management application is not supported in a network address translation (NAT) environment where the server and client are on different sides of the NAT server.

Management application has the following client and server system requirements:

- In the Professional edition, a single server supports a single client, which must be a local client only.

- In Professional Plus and Enterprise editions, a single server supports a maximum of 25 clients, which can be local or remote on 64-bit servers. To support more than 8 clients, you must make the following changes to your configuration:
  - Increase the server memory size. You can configure the server memory size from the **Options** dialog box > **Memory Allocations** pane. For instructions, refer to a Brocade Network Advisor user manual or to online help.
  - Increase the PostgreSQL database shared buffers memory allocation to 1024 MB by editing the `Install_Home\data\databases\postgresql.conf` file.

Downloading the software

You can download the software and documentation from the MyBrocade website.

1. Go to the MyBrocade website.

   http://my.brocade.com/
2. Enter your user ID and password.

   If you do not already have a MyBrocade account, you can create one.
3. Select **MyBrocade** from the **Take me to** list, if necessary.
4. Click **LOG IN**.
5. Click **downloads** on the main page.
6. Select **Management Software** from the **Download by** list.
7. Click **Management application** in the **Product Name** list.
8. Select the highest version number for the latest GA code.

   For example, click **Network Advisor 14.4.2**, and then click **Network Advisor 14.4.2 Brocade GA.**

   To download the documentation, click **Network Advisor 14.4.2 Manuals**, and then select the manual that you want to download.
9. Select one of the following links to download the software:
   - Network Advisor 14.4.2 GA for Windows
   - Network Advisor 14.4.2 GA for Linux

   You can also access the release notes and the MD5 checksum from this location.
10. Read the **Export Compliance**, select the certification check box, and click **Submit**.
11. Read the **Brocade End User License Agreement**, and click **I Accept**.
12. Click **Save** on the **File Download** dialog box.
13. Browse to the location where you want to save the software, and click **Save**.

Preinstallation requirements

Before you install Management application, make sure that you meet the following requirements:

- Make sure that all system requirements have been met before installation. For specific system requirements, refer to System requirements on page 11.
- To avoid errors, close all instances of the application before beginning the installation or uninstallation procedures.

For a UNIX system, if you still receive error messages after closing the application, enter the following commands:

- **#ps -ef | grep -i ""** to list the process IDs.
- **#kill -9 "** *Process_ID* **"** where *Process_ID* is any Management application process.

Additional preinstallation requirements for UNIX systems

- Make sure that an X Server is available for display and is configured to permit X Client applications to display from the host on which they are installing the Management application server (typically, this simply requires that the systems console be present and running with a logged-in user on the X Server-based desktop session, such as KDE, or GNOME).

  If this is a headless unit with no console, refer to Additional preinstallation requirements for UNIX systems (headless installation) on page 23.
- Make sure that the DISPLAY environment variable is correctly defined in the shell with a valid value (for example, to display to the local console, **export DISPLAY=:0.0**, or to display to a remote system that has an X Server running, **export DISPLAY=** *Remote_IP_address***:0.0**).

  You may also need to consider a firewall that might block the display to the X Server, which listens by default on TCP port 6000 on the remote host.

  To display to a remote system, you need to permit the remote display of the X Server by running the **xhost +IP** command, where IP is the IP address of the Management application server host from the X-based desktop of the remote system.
- Make sure that you test the DISPLAY definition by running the **xterm** command from the same shell from which you run **install.bin**. A new X terminal window to the destination X Server display should open.
- For Linux OS with the SELinux security policy enabled, make sure that you complete the following steps:
  1. Disable the SELinux security policy using the **setenforce 0** command.
  2. Install the application (refer to Installing the application on page 20).
  3. Enable the SELinux security policy using the **setenforce 1** command.

Troubleshooting Linux SUSE 11.3

1. CASE 1: Follow these steps to troubleshoot when the installation fails with an error saying "`error while loading shared libraries: libreadline.so.6: cannot open shared object file: No such file or directory`".
   - Install libreadline.so.6.
   - Launch the terminal.
   - Enter the following:
     - **wget.http://download.opensuse.org/distribution/11.3/repo/oss/suse/x86_64/libreadline6-6.1-8.1.x86_64.rpm.**
     - **rpm -Uvh libreadline6-6.1-8.1.x86_64.rpm --replacepkgs.**
     - **libreadline.so.6, libreadline.so.6.1 will be created in /lib64 folder.**
   - Install the application (refer to Installing the application on page 20).

2. CASE 2: Follow these steps to troubleshoot when the installation fails with an error saying "`mysql: symbol lookup error: /usr/local/lib/libreadline.so.6: undefined symbol: UP`".
   - Copy libreadline.so.6.1 and libreadline.so.6 from /lib64 to /usr/local/lib.
   - cp /lib64/libreadline.so.* /usr/local/lib.
   - cd /usr/local/lib.
   - Enter #ldconfig.
   - Enter #apt-get update.
   - Install the application (refer to Installing the application on page 20).

Prerequisites for starting SLP services in Linux servers

To start SLP services in Linux servers, Linux servers must be installed with the following libraries:

- Linux-vdso.so.1
- Libcrypto.so.1.0.0
- Libpthread.so.0
- Libm.so.6
- Libc.so.6
- Libdl.so.2
- Libz.so.1
- Ld-linux-x86-64.so.2

Follow these steps to install the libraries:

1. Install glibc. To install libc.so.6, libdl.so.2, libpthread.so.0, linux-vdso.so.1, libm.so.6, and ld-linux.so.2, use the **yum install glibc** command.
2. Install zlib. To install libz.so.1, use the **yum install zlib** command.
3. Install OpenSSL. To install ibcrypto.so.6, use the **yum provides libcrypto.so.6** command. This command lists the compatible packages; you can install any of the packages using the **yum install** *package* command. For example, **yum install** openssl098e-0.9.8e-29.el7_2.3*.

   NOTE
   The above libraries are compatible with both 32-bit and 64-bit, as the SLP service is 32-bit.
   Beginning with version 14.0.0, the 32-bit Installer is not supported.

Installing the application

Before you install the application, make sure that your system meets the minimum preinstallation requirements (refer to Preinstallation requirements on page 18). If you are migrating data, refer to Installation on page 11.

NOTE
Beginning with version 14.3.1 release, only SAN installation is supported.

NOTE
On Windows systems, you must be an administrator with read and write privileges to install Management application.

NOTE
On UNIX systems, you must be the root user to install Management application.

To install the new application version, complete the following steps.

1. Choose one of the following options:
   - For Windows systems, navigate to the *Download_Location* \ *Application_Name* \windows\install.exe file, and select **Run as administrator**.
   - For UNIX systems, complete the following steps:
     1. On the Management application server, navigate to the following directory: *Download_Location* / *Application_Name* / *UNIX_Platform* /bin
     2. Type the following at the command line: `ulimit -n 2000`
     3. Type the following at the command line: `./install.bin` or `sh install.bin`

        NOTE
        On Linux systems, if you double-click the install.bin file, select **Run**. Do not select **Run in Terminal**.
2. Click **Next** on the **Introduction** window.
3. Read the agreement on the **License Agreement** window, select **I accept the terms of the License Agreement**, and click **Next**.
4. Select the usual location for your system application files (for example, D:\Program Files\ *Application_Name* or opt/ *Application_Name*) on the **Select Install Folder** window and click **Next**.

   NOTE
   Do not install to the root directory C:\ (Windows) or /root (UNIX).
5. Review the displayed installation summary on the **Pre-Installation Summary** window, and click **Install**.

6. Make sure that the **Launch Configuration** check box is selected (default) on the **Installation Complete** window, and click **Done**.

   NOTE
   If a minimum of 10 GB space is not available on your server during installation, a warning message displays and the installation fails.

   If the local host is not mapped to the loopback address, an error message displays. You must map the loopback address to the local host (refer to Mapping the loopback address to the local host on page 22) before you configure the application.

   If the local host is mapped to the loopback address, the configuration wizard displays. To configure the application, refer to one of the following sections:

   - If this is a fresh installation, refer to Installation on page 11.
   - If you are upgrading from a previous version and need to migrate data, refer to Installation on page 11.

   For Linux systems, the following lists the folder permissions configured during installation:

   - Install_Home: 775
   - conf: 775
   - conf/schema folder (including subfolders): 775
   - data/database: 700
   - db (including subfolders): 775
   - temp: 775
   - support: 777
   - All other folders: 774

Mapping the loopback address to the local host

To map the loopback address to the local host, complete the following steps.

1. Open the hosts file.

   For Windows, the hosts file is located in the WINDOWS\system32\drivers\etc directory.

   For Linux, the hosts file is located in the /etc directory.

2. Add the following entries:

```
# For IPv4 machine
127.0.0.1          localhost
# For IPv6 enabled machine
127.0.0.1       localhost
::1             localhost
```

3. Save and close the file.

   To configure the application, refer to one of the following sections:

   - If this is a fresh installation, refer to Installation on page 11.
   - If you are upgrading from a previous version and need to migrate data, refer to Installation on page 11.

Headless installation

Headless installation, also known as **silent mode installation**, is fully supported on all platforms. Once initiated, the headless installation requires minimal user interaction and runs based on the default values provided. Headless installation performs the actual installation; however, you must use the configuration wizard in graphical user interface mode to copy data and settings, configure the FTP or SCP server, configure IP, and configure server ports.

Make sure that all system requirements have been met before to installation. For specific system requirements, refer to System requirements on page 11.

Additional preinstallation requirements for UNIX systems (headless installation)

To run the initial configuration, an X Server display is required, even when performing a headless installation. Before you install Management application, complete the following:

- Make sure that an X Server is available for display and is configured to permit X Client applications to display from the host on which they are installing the Management application server (typically, this simply requires that the system console be present and running with a logged-in user on the X Server-based desktop session, such as KDE and GNOME.
  - The DISPLAY can be any host X Server (for example, DISPLAY can be set to display the configuration to another UNIX system that has an X-based desktop).
- Make sure that the DISPLAY environment variable is correctly defined in the shell with a valid value (for example, to display to the local console, **export DISPLAY=:0.0**, or to display to a remote system that has an X Server running, **export DISPLAY=** *Remote_IP_Address***:0.0**).
  - To display to a remote system, you must permit the remote display of the X Server by running the **xhost +IP** command, where IP is the IP address of the Management application server host, on a local terminal window of the X-based desktop of the remote system.
  - You may also need to consider a firewall that may block the display to the X Server, which listens by default on TCP port 6000 on the remote host.
- Make sure that you test the DISPLAY definition by running the **xterm** command from the same shell from which you run install.bin. A new X terminal window to the destination X Server display will open.

Performing a headless installation on Windows and Linux systems

To perform a headless installation through the CLI, download the software (refer to Downloading the Software).

- For Windows systems, complete the following steps:
  1. Select **Start** > **Programs** > **Accessories**, right-click **Command Prompt**, and select **Run as administrator**.
  2. Issue the following command:

     ```
     install.exe -i silent - DHEADLESS_CONFIGURATION="headless-installation.properties filepath" "-DHEADLESS=true”
     ```
- For Linux systems, open a Linux shell, and issue this command:

  ```
  sh install.bin -i silent "-DHEADLESS_CONFIG_MODE=false"
  ```

  ```
  sh configwizard "-DHEADLESS_CONFIGURATION=/opt/headless-installation.properties" "-DHEADLESS=true"
  ```

The application installs in silent mode using default settings.

To configure the application, refer to one of the following sections:

- If this is a fresh installation, refer to Installation on page 11.
- If you are upgrading from a previous version and need to migrate data, refer to Installation on page 11.

Troubleshooting the Linux headless installation

If you have completed all of the preinstallation requirements and you are still unable to install the application, run the following commands on the host.

1. Go to *Install_Home* / (the directory containing install.bin).
2. Issue `strace -f -F -v -s 1024 -o NetworkAdvisorinstall.txt ./install.bin`.
3. Issue `rpm -qa >> system.txt`.
4. Issue `ps -elf >> system.txt`.
5. Issue `md5sum install.bin >> system.txt`.
6. Issue `df -k >> system.txt`.
7. Issue `sh -c "xterm -e echo nothing >> system.txt 2>&1"`.
8. Execute `env >> system.txt` .
9. Execute `sh -c "DISPLAY=:0.0 xterm -e echo nothing >> system.txt 2>&1"`.
10. Execute `zip support1.zip NetworkAdvisorinstall.txt system.txt`.

    Send the support1.zip file output (containing install.txt and system.txt) to Technical Support. This file will help Technical Support isolate the issue.

Collecting supportSave information on Windows and Linux

To collect server supportSave information, run the script file located at `<BNA_HOME>\bin\commandsupportsave`. Once the script file is triggered, the server supportsave information is collected at `<BNA_HOME>\support`.

Client-only installation

You can install a client-only application on a machine other than the server (without using a web browser) by creating a client bundle on the server and then copying and installing that client on another machine.

Installing the client-only application

The client bundle is supported on a 64-bit OS only. The download client is bundled with the Management application server Java runtime environment package. To download the client bundle, the browser operating system and the server operating system must be the same.

1. Click the client bundle, and download the file.
2. Extract the client bundle in the following path: "C:\Program Files".

3. Navigate to the extract_location\bin directory, and run the appropriate .bat file.
   - For Windows, navigate to C:\Users\ *user_name*\desktop\windows-clientbundle\bin, and run `dcmclient.bat`.
   - For Linux, navigate to opt/linux-clientbundle/bin, and run `dcmclient`.

   If you modify the data in the **Options** dialog box, the client bundle must be triggered manually.
   - For Windows, navigate to Install_Home\bin, and run `create-client-bundle.bat`.
   - For Linux, navigate to Install_Home\bin, and run `create-client-bundle`.

   The **Management application Log In** dialog box displays.

   NOTE
   If the default starting port number is changed to some other port number, you must restart the server, regenerate the client bundle, and then download the client bundle to launch the client.

4. Enter the IP address of the Management application server in the **Network Address** list.

   NOTE
   The server must have the exact same version, edition, starting port number, and network size as the client.

   NOTE
   You can remove a server from the **Network Address** list by selecting the IP address and clicking **Delete**.

5. Enter your user name and password.

   The defaults are Administrator and password.

   NOTE
   Do not enter *Domain**User_Name* in the **User ID** field for LDAP server authentication.

6. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
7. Click **Login**.
8. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Management Application Configuration

Configuring Management application

If you have not installed the application, refer to Installation on page 11. If you are migrating data, refer to Data Migration on page 51.

To configure Management application, complete the following steps.

1. Click **Next** on the **Welcome** window.
2. Click **No, don't copy any data and settings** (default) on the **Copy Data and Settings (Migration)** window, and click **Next**.

   NOTE
   You cannot migrate data from an earlier release of Management application to 14.4.2 after you complete the 14.4.2 configuration.

   To migrate data from a previous management application version, refer to Data Migration on page 51 .
3. Select one of the following options on the **Package** window, and click **Next**.
   - **SAN with SMI Agent** (default)
   - **SMI Agent Only**

     NOTE
     SMI Agent is not supported in a Professional edition configuration.

     NOTE
     If you choose to install only the SMI Agent, the configuration defaults to the SAN Enterprise package. When you open the Management application client, a **License** dialog box displays, where you must enter a SAN Enterprise license key to use the client. If you enter a SAN Professional Plus license key, you must downgrade your license and restart all services for the changes to take effect. For instructions, refer to the user manual or online help.

4. Select one of the following options on the **Installation Type** window, and click **Next**.

   NOTE
   SAN768B, SAN768B-2, SAN256B-6, and SAN512B-6 Chassis require the Enterprise edition.

   - **Management application - Licensed version** (default)

     Requires you to enter a license key during configuration to enable features and configuration.

   - **Management application - 120 days Trial**

     The trial edition enables you to manage SAN from a single interface for 120 days.

     Enables you to manage IP networks from a single interface for 120 days.

     ATTENTION
     If you choose to install the Trial option, once the trial period ends (120 days), you must upgrade to Licensed software.

   - **Management application - Professional**

     The Professional edition is bundled with Fabric OS devices to manage small SAN from a single interface. SMI Agent is not available with the Professional edition.

5. (Licensed software only) If you are installing Licensed software, browse to the license file (.xml), and click **Next** on the **Server License** window.

   You can also copy (**Ctrl+C**) and paste (**Ctrl+V**) the license key into the **License Key** field. The **License Key** field is not case-sensitive.

6. Complete the following steps on the **FTP/SCP/SFTP Server** window.
   a) Choose one of the following options:
      - Select **Built-in FTP/SCP/SFTP Server** (default) to configure an internal FTP, SCP, or SFTP server, and select one of the following options:
        - Select **Built-in FTP Server** to configure an internal FTP server This is the default option. The internal FTP server uses a default account and port 21. You can configure your own account from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor User Manual or to online help.
        - Select **Built-in SCP/SFTP Server** to configure an internal SCP or SFTP server The internal SCP or SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor User Manual or to online help.
      - Select **External FTP/SCP/SFTP Server** to configure an external FTP server. You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor User Manual or to online help.
   b) Click **Next**.

      If port 21 or 22 is busy, a message displays. Click **OK** to close the message, and continue. Once the Management application is configured, make sure that port 21 or 22 is free, and restart the server to start the FTP/SCP/SFTP service.

      NOTE
      If you use an FTP, SCP, or SFTP server that is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.

      NOTE
      If port 22 is occupied, the following details are the workaround for Linux,

      - To find all processes, issue the following command: `Kill -9 <PID>`.
      - If SCP and SFTP services are already running, issue the following command: `lsof -i tcp:22` and terminate the process with the same id running in both IPv4 and IPv6 in SSHD services.
      - If FTP services are already running, issue the following command: `lsof -i tcp:21` and terminate the process with the same id running in both IPv4 and IPv6 FTP services.
      - If Database services are already running, issue the following commands:

        ```
        lsof -i tcp:5432
        kill -9 <pidofthatprocess>
        ```

      For windows:

      - To find all processes running in FTP(21), SCP(22), and Database(5432), issue the following command: `netstat -aon` and terminate the process by issuing the following command: `taskkill /F /PID <processid>`.

7. Configure the database password on the **Database Administrator Password (dcmadmin)** window by completing the following steps.
   a) Choose one of the following options:
      - To use the default password, select **Default password**. This is the default option. The default is password.
      - To configure a new password, select **New password** and enter a new password in the **Password** and **Confirm Password** fields. The password must be between 8 and 15 alphanumeric characters. Special characters except the single quote (') are allowed.

   b) Click **Next**.

      You can configure the external FTP server settings from the **Options** dialog box.

8. Complete the following steps on the **Server IP Configuration** window.

   NOTE
   If the Management server or client has multiple network interface cards and if any interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:

   Server impact

   - Configuration wizard (does not display all IP addresses)
   - Trap and syslog auto-registration
   - Report content (Ipconfiguration element does not display all server IP addresses)
   - Trace dump through FTP

   Client impact

   - **Options** dialog box (does not display all IP addresses)
   - **Firmware import and download** dialog box
   - Firmware import for Fabric OS products
   - **FTP** button in the **Technical Support Repository** dialog box
   - Technical supportSave of Fabric OS and host products through FTP

   a) Select an address from the **Server IP Configuration** list.

      NOTE
      For Professional software, the **Server IP Configuration** address is set to "localhost" by default. You cannot change this address.

      NOTE
      For SMI Agent, if the **Server IP Configuration** list contains a duplicate IP address or is empty, an error message displays and the configuration wizard closes.

      NOTE
      If the "host name" contains invalid characters, the host name does not display in the list. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default.

      If Domain Name System (DNS) is not configured for your network, do not select the "hostname" option from the **Server IP Configuration** list. Selecting the "hostname" option prevents clients and devices from communicating with the server.

   b) Select an address from the **Switch - Server IP Configuration Preferred Address** list.

      Select **Any** from the **Switch - Server IP Configuration Preferred Address** list to enable switch and server communication with one of the reachable IP addresses present in the server. By default, the **Any** option is selected.

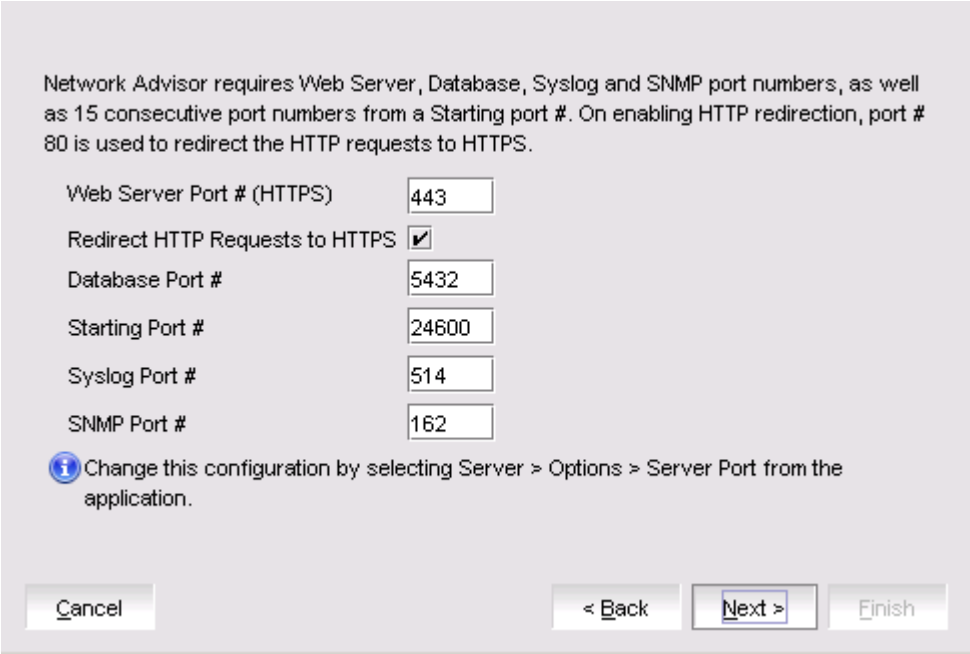
      or

      Select an IP address from the **Switch - Server IP Configuration Preferred Address** list. The preferred IP address is used for switch and server communication. If the selected IP addresses changes, you will be unable to connect to the server. To change the IP address after configuration, refer to Configuring an explicit server IP address on page 47.

   c) Click **Next**.

9. Complete the following steps on the **Server Configuration** window.

FIGURE 1 Server Configuration window



a) Enter a port number in the **Web Server Port # (HTTPS)** field (default is 443).

b) Enable HTTP redirection to HTTPS by selecting the **Redirect HTTP Requests to HTTPS** check box.

When you enable HTTP redirection, the server uses port 80 to redirect HTTP requests to HTTPS. You can configure the server port settings from the **Options** dialog box (**Server Port** pane). For instructions, refer to a Brocade Network Advisor User Manual or to online help.

c) Enter a port number in the **Database Port #** field (default is 5432).

NOTE
Do not use a port number below 1024.

d) Enter a port number in the **Starting Port #** field (the default is 24600). If the default port is changed to some other port number, restart the server, regenerate the client bundle running the `<BNA-Install-Location>\bin\create-client-bundle.bat` file, and download the client-bundle to launch the client.

NOTE
For Professional software, the server requires 11 consecutive free ports beginning with the starting port number.

NOTE
For Trial and Licensed software, the server requires 11 consecutive free ports beginning with the starting port number.

e) Enter a port number in the **Syslog Port #** field (default is 514).

NOTE

If the default syslog port number is already in use, you will not receive syslog messages from the device. To find and stop the process currently running on the default syslog port number, refer to Syslog troubleshooting on page 40.

f) Enter a port number in the **SNMP Port #** field (default is 162).

g) Click **Next**.

If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** window, and edit the syslog port number. Click **Yes** to close the message.

If you enter a port number already in use, a warning displays next to the associated port number field. Edit that port number, and click **Next**.

10. (SAN with SMI Agent) Complete the following steps on the **SMI Agent Configuration** window.

a) Enable the SMI Agent by selecting the **Enable SMI Agent** check box.

b) Enable SLP by selecting the **Enable SLP** check box, if necessary.

SLP is enabled only after you select the **Enable SMI Agent** check box.

c) Enable SSL by selecting the **Enable SSL** check box, if necessary.

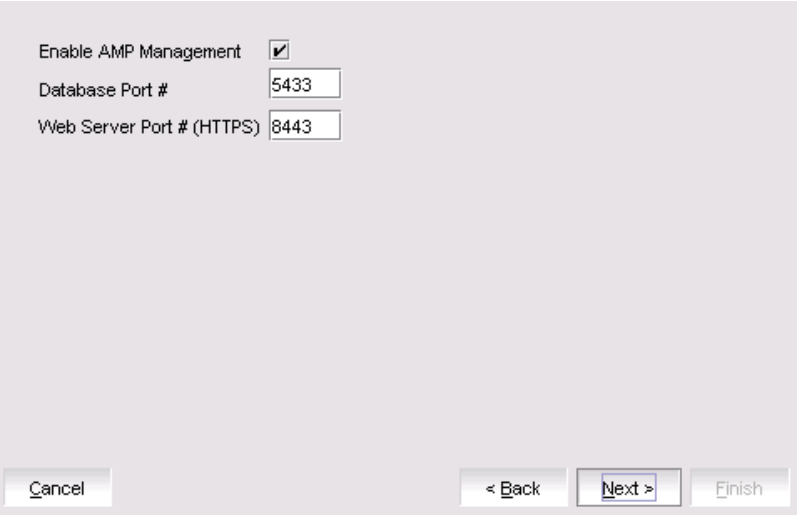
SSL is enabled only after you select the **Enable SMI Agent** check box.

d) Enter the SMI Agent port number in the **SMI Agent Port #** field (default is 5989 if **Enable SSL** is selected; otherwise, the default is 5988).

e) Click **Next**.

11. (SAN with AMP Management)Complete the following steps on the **AMP Management** window.

FIGURE 2 AMP Management



a) Enable the AMP by selecting the **Enable AMP Management** check box.

The **Database Port#** and **Web Server Port# (HTTPS)** fields display the default port numbers.

The default port number for the **Database Port#** field is **5433** and for the **Web Server Port# (HTTPS)** field is **8443**.

b) Click **Next**.

12. (SAN Enterprise or SMI Agent) Select one of the following options on the **SAN Network Size** screen and click **Next**:

    NOTE
    Port count is equal to the total number of switch ports across all fabrics.

    - **Small (managing up to 2000 switch ports, 1-20 domains)**
    - **Medium (managing up to 5000 switch ports, 21-60 domains)**
    - **Large (managing up to 15000 switch ports, 61-120 domains)**

    If you are configuring IP Enterprise, continue with Configuring Management application; otherwise, go toConfiguring Management application.

    The **Database Port#** and **Web Server Port# (HTTPS)** fields displays the default port numbers.
13. Enable feature usage data transfer from the application by selecting the **Yes, I want to participate** option.

    If you do not want to participate in feature usage data transfer, make sure the **No, Thank You** option is selected. You can stop participating at any time. To view an example of the usage data, click **View Example Data**.

    To stop participating in feature usage data transfer after configuration, refer to *Product improvement*.
14. Verify your configuration information on the **Server Configuration Summary** window, and click **Next**.
15. Click **Finish** on the **Start Server** window.

    After all of the services are started, the **Log In** dialog box displays.

    To make changes to the configuration, you can relaunch the configuration wizard (refer to Configuring an explicit server IP address on page 47).
16. Complete the following steps on the **Start Server** screen.
    a) (Trial and Licensed only) Select the **Start SMI Agent** check box, if necessary.

       The **Start SMI Agent** check box is enabled only if you enabled the SMI Agent on the **SMI Agent Configuration** window.
    b) (Trial and Licensed only) Select the **Start SLP** check box, if necessary.

       The **Start SLP** check box is enabled only if you enabled SLP on the **SMI Agent Configuration** window.
    c) Select the **Start Client** check box, if necessary.

       The **Start Client** check box displays only if you selected SAN with SMI Agent on the **Package** window.
    d) Click **Finish**.

       After all of the services are started, the **Log In** dialog box displays.

       To make changes to the configuration, you can relaunch the configuration wizard (refer to Configuring an explicit server IP address on page 47).
17. Enter your user name and password.

    The defaults are Administrator and password.

    NOTE
    Do not enter Domain\User_Name in the **User ID** field for LDAP server authentication.

18. Click **Login**.
19. Click **OK** on the Management application login banner.

Accessing the Management application interfaces

Use the following procedures to access Management application from the server and client as well as to access the Server Management Console and the SMI Agent Configuration Tool.

Logging in to a server

You must log in to a server to monitor your network.

NOTE
To log in, you must have an established user account on the server.

1. Double-click the desktop icon, or open the application from the **Start** menu.

   The **Log In** dialog box displays.

2. Log in to another server by entering its IP address in the **Network Address** field.

   NOTE
   The server must have the exact same version, edition, starting port number, and network size as the client.

   NOTE
   Remove a server from the **Network Address** list by selecting the IP address and clicking **Delete**.

3. Enter your user name and password.

   The defaults are Administrator and password.

   NOTE
   Do not enter Domain\User_Name in the **User ID** field for LDAP server authentication.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Launching a remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache. To clear the previous version, refer to Clearing previous versions of the remote client on page 36.

The remote client requires Oracle JRE. For the currently supported JRE version for Management application, refer to the release notes. For the website that lists patch information, go to http://www.oracle.com/technetwork/java/javase/downloads/index.html.

NOTE
For higher performance, use a 64-bit JRE.

1. Choose one of the following options:
   - Open a web browser, and enter the IP address of the Management application server in the **Address** bar.
   - If the web server port number does not use the default (443 if SSL is enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address; for example, *IP_Address*:*Port_Number*.
   - If this is the first time you are accessing this version of Management application, a **Start** menu shortcut is automatically created in the Management application program directory.

     For Linux systems, remote client shortcuts are not created.
   - Select **Management application (Server_IP_Address)** in the Management application directory from the **Start** menu.

     The Management application web client login page displays.
2. Click **Desktop Client**.

   The Management application web start page displays.
3. Click the Management application web start link.

   The **Log In** dialog box displays.
4. Log in to another server by entering its IP address in the **Network Address** field.

   NOTE
   The server must have the exact same version, edition, starting port number, and network size as the client.

   NOTE
   You can remove a server from the **Network Address** list by selecting the IP address and clicking **Delete**.
5. Enter your user name and password.

   The defaults are Administrator and password.

   NOTE
   Do not enter Domain*User_Name* in the **User ID** field for LDAP server authentication.

6. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
7. Click **Login**.
8. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Clearing previous versions of the remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache.

To clear the Java cache, complete the following steps.

1. Select **Start > Settings > Control Panel > Java**.

   The **Java Control Panel** dialog box displays.

2. Click **View** on the **General** tab.

   The **Java Cache Viewer** dialog box displays.
3. Right-click the application, and select **Delete**.
4. Click **Close** on the **Java Cache Viewer** dialog box.
5. Click **OK** on the **Java Control Panel** dialog box.

   To create a remote client link in the **Start** menu, refer to Launching a remote client on page 35.

Launching the SMC on Windows

Open the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a shortcut.

Launching the SMC on Linux

NOTE
The Server Management Console is a graphical user interface and should be launched from the XConsole on Linux systems.

Double-click the SMC icon on your desktop.

Or

1. On the Management application server, go to the following directory:

   Install_Directory /bin
2. Type the following at the command line:

```
./smc
Or
sh smc
```

Launching the SMIA Configuration Tool

1. Launch the **Server Management Console** from the **Start** menu.
2. Click **Configure SMI Agent**.

   The **SMIA Configuration Tool Log In** dialog box displays.
3. Enter your user name and password.

   The defaults are Administrator and password.
4. Click **Login**.

Launching the SMIA Configuration Tool remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache. To clear the previous version, refer to Clearing previous versions of the remote client on page 36.

The remote client requires Oracle JRE. For the currently supported JRE version for Management application, refer to the release notes. For the website listing patch information, go to http://www.oracle.com/technetwork/java/javase/downloads/index.html.

1. Choose one of the following options:
   - Open a web browser, and enter the IP address of the Management application server in the **Address** bar.
   - If the web server port number does not use the default (443 if SSL is enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address; for example, *IP_Address*:*Port_Number*.
   - If this is the first time you are accessing this version of Management application, a **Start** menu shortcut is automatically created in the Management application program directory.

     For Linux systems, remote client shortcuts are not created.
   - Select *Management application (Server_IP_Address)* in the Management application directory from the **Start** menu.

     The Management application web client login page displays.
2. Click **Desktop Client**.

   The Management application web start page displays.
3. Click the **SMIA Configuration Tool** web start link.

   The **SMIA Configuration Tool Log In** dialog box displays.
4. Enter your user name and password.

   The defaults are Administrator and password.
5. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
6. Click **Login**.

   The **SMIA Configuration Tool** displays.

Performance collection for SMI-A only

For SMI-A only installations, you can use the following procedures to configure performance collection using scripts.

Enabling or disabling performance statistics collection

To enable or disable performance statistics collection, complete the following steps.

1. On Windows systems, complete the following steps.
   a) Open a command prompt, and navigate to the Install_Home\utilities directory.
   b) Enable performance statistics collection by typing **sanperformancestatsenable.bat** *db_username db_password* **enable** and pressing **Enter**. For example, **`sanperformancestatsenable.bat dcmadmin passw0rd enable`**.

   Disable performance statistics collection by typing **sanperformancestatsenable.bat** *db_username db_password* **disable** and pressing **Enter**.

2. On UNIX systems, complete the following steps.
   a) Open a terminal, and navigate to the Install_Home\utilities directory.
   b) Enable performance statistics collection by typing **sanperformancestatsenable** *db_username db_password* **enable** and pressing **Enter**. For example **`ssanperformancestatsenable dcmadmin passw0rd enable`**.

   Disable performance statistics collection by typing **sanperformancestatsenable** *db_username db_password* **disable** and pressing **Enter**.

Updating system threshold data

To configure the SMI-A only installation to update the file system threshold data in the system property table, complete the following steps:

1. On Windows systems, complete the following steps:
   a) Open a command prompt, and navigate to the Install_Home\utilities directory.
   b) Update file system threshold data by typing **updatethresholddata.bat** *db_username db_password* THRESHOLD_WARN THRESHOLD_RISK THRESHOLD and pressing **Enter**. For example, **`updatethresholddata.bat dcmadmin passw0rd 80 90 95`**.
2. On UNIX systems, complete the following steps:
   a) Open a terminal, and navigate to the Install_Home\utilities directory.
   b) Update file system threshold data by typing **updatethresholddata** *db_username db_password* THRESHOLD_WARN THRESHOLD_RISK THRESHOLD and pressing **Enter**.

Exporting configuration data

To export configuration data from the CFG_backup_archive table, complete the following steps:

1. On Windows systems, complete the following steps:
   a) Open a command prompt, and navigate to the Install_Home\utilities directory.
   b) Export configuration data by typing **exportconfigdata.bat** *db_username db_password* and pressing **Enter**. For example, **exportconfigdata.bat dcmadmin passw0rd**.
2. On UNIX systems, complete the following steps:
   a) Open a terminal, and navigate to the Install_Home\utilities directory.
   b) Export configuration data by typing **exportconfigdata** *db_username db_password* and pressing **Enter**. For example, **exportconfigdata dcmadmin passw0rd**.

Clearing performance data

To clear performance data (all time series child table data), complete the following steps:

1. On Windows systems, complete the following steps:
   a) Open a command prompt, and navigate to the Install_Home\utilities directory.
   b) Clear performance data by typing **clear-performance-data.bat** *db_username db_password* and pressing **Enter**. For example, **clear-performance-data.bat dcmadmin passw0rd**.

2. On UNIX systems, complete the following steps:
   a) Open a terminal, and navigate to the Install_Home\utilities directory.
   b) Clear performance data by typing **clear-performance-data** *db_username db_password* and pressing **Enter**. For example, **clear-performance-data dcmadmin passw0rd**.

Syslog troubleshooting

If the default syslog port number is already in use, you will not receive any syslog messages from the device. Use the following procedures to determine which process is running on the syslog port and to stop the process.

Finding the process

1. Open a command window.
2. Choose one of the following options:
   - On Windows systems, type **netstat -anb | find /i "514"** or **netstat -aon**, and press **Enter**.

     The process running on port 514 displays.

     Example output: `UDP 127:0:0:1:514 *:* 3328`.
   - On Linux systems, type **netstat -nap | grep 514** or **ps -afx**, and press **Enter**.

     The process running on port 514 displays.

     Example output: `UDP 0 0 ::ffff:127:0:0:1:514 :::* 27397`.

Stopping the process

Choose one of the following options:

- On Windows systems, type **taskkill /F /PID "***ProcessID* **"**, where *ProcessID* is the ID of the process that you want to stop, and press **Enter**.

  For example, **taskkill /F /PID "3328"**.

  Or

  - Select **Ctrl + Shift + Esc** to open Windows Task Manager.
  - Click the **Processes** tab.
  - Click the **PID** column header to sort the processes by PID.
  - Select the process that you want to stop, and click **End Process**
- On Linux systems, type **kill -9 "***ProcessID* **"**, where *ProcessID* is the ID of the process that you want to stop, and press **Enter**.

  For example, **kill -9 "27397"**.

Installing the ODBC driver

You must have the Open Database Connectivity (ODBC) driver to allow remote clients to export data and generate reports. The ODBC driver enables you to configure the data source name (DSN) for the Management application database.

Installing the ODBC driver on Windows systems

To install the ODBC driver, complete the following steps.

1. Double-click **edb_psqlodbc.exe** located on the DVD (*DVD_Drive*/Management application/odbc/Windows).
2. Install the file to the usual location for your system's application files (for example, C:\Program Files\Management application ODBC Driver) on the **Select Install Folder** window, and click **Next**.

   NOTE
   If you select an invalid location, the ODBC driver is installed in a different location than where the ODBC executable drivers are located.

3. On the **Ready to Install** window, click **Next**.
4. Click **Finish** to complete the installation.

Adding the data source on Windows systems

To add the data source, complete the following steps.

1. Select **Start** > **Settings** > **Control Panel** > **Administrative Tools**.
2. Right-click **Data Sources (ODBC)**, and select **Run as administrator**.

   The **ODBC Data Source Administrator** dialog box displays. If the **ODBC Data Source Administrator** dialog box does not display, select **Start > Run**, type **%windir%\SysWOW64\odbcad32.exe**, and press **Enter**.
3. Click the **System DSN** tab.
4. Click **Add**.

   The **Create a New Data Source** dialog box displays.
5. Select **PostgreSQL Unicode**.
6. Click **Finish**.

   The **PostgreSQL Unicode ODBC Driver (psqlODBC) Setup** dialog box displays.
7. Enter a name for the data source in the **Datasource** field.
8. Enter the description of the Management application database in the **Description** field.
9. Enter the name of the Management application database in the **Database** field.
10. Select **enable** or **disable** from the **SSL Mode** list to specify whether to use SSL when connecting to the database.
11. Enter the IP address or host name of the Management application server in the **Server** field.
12. Enter the database server port number in the **Port Number** field.
13. Enter the database user name in the **User Name** field.
14. Enter the password in the **Password** field.
15. Click **Test** to test the connection.

    NOTE
    You can also use the Windows ODBC Driver Manager to add the DSN for the Linux database server.

16. Click **OK** on the **Connection Test** dialog box.
17. Click **Save**.
18. Click **OK** on the **ODBC Data Source Administrator** dialog box.

Installing the ODBC driver on Linux systems

You must have the Open Database Connectivity (ODBC) driver to allow remote clients to export data and generate reports. The ODBC driver enables you to configure the data source name (DSN) for the Management application database.

To install the ODBC driver, complete the following steps.

1. Issue the following command in the terminal:

```
> su
> chmod 777 edb_psqlodbc.bin
> ./edb_psqlodbc.bin
```

   For 64-bit Linux systems, the installer file is located in DVD/Management application/odbc/Linux_64/psqlodbc.bin.

2. On the **Setup psqlODBC** window, click **Next**.
3. Install the file to the usual location for your system's application files (for example, /opt/PostgreSQL/psqlODBC) on the **Installation Directory** window, and click **Next**.

   NOTE
   If you select an invalid location, the ODBC driver is installed in a different location than where the ODBC executable drivers are located.

4. On the **Ready to Install** window, click **Next**.
5. On the **Completing the psqlODBC Setup Wizard** window, click **Finish** to complete the installation.

Adding the data source on Linux systems

Before you edit the INI files, install Management application (refer to Installation on page 11), and make sure that the PostgreSQL database is up and running.

NOTE
For Red Hat and Oracle Enterprise systems, the odbc.ini and odbcinst.ini files are located in /etc. For SUSE systems, the odbc.ini and odbcinst.ini files are located in /etc/unixODBC.

1. Open the odbc.ini file in an editor, and enter the following data source information:

```
[TestDB]
Description = PostgreSQL 9.5.1
Driver = /opt/PostgreSQL/psqlODBC/lib/psqlodbcw.so
Database = dcmdb
Servername = 172.26.1.54
UserName = dcmadmin
Password = passw0rd
Port = 5432
```

2. Save and close the odbc.ini file.
3. Open the odbcinst.ini file in a text editor, and make sure that the driver path information is correct.

   After you install the PostgreSQL ODBC driver, the odbcinst.ini file should automatically update the driver path. If the driver path is not updated, enter the following information:

```
[psqlODBC]
Description=PostgreSQL ODBC driver
Driver=/opt/PostgreSQL/psqlODBC/lib/psqlodbcw.so
```

4. Save and close the odbcinst.ini file.

Testing the connection on Linux systems

To test the connection, complete the following steps.

1. Download and install Open Office.
2. Select **File** > **New** > **Database**.

   The **Database Wizard** displays.
3. On the **Select database** window, complete the following steps.
   a) Select the **Connect to an existing database** option.
   b) Select **ODBC** from the list.
   c) Click **Next**.
4. On the **Set up ODBC connection** window, complete the following steps.
   a) Click **Browse**.

      The data source saved in the odbc.ini file is populated in the **Datasource** dialog box.
   b) Select the data source, and click **OK** on the **Datasource** dialog box.
   c) Click **Next**.
5. On the **Set up user authentication** window, complete the following steps.
   a) Enter the database user name in the **User name** field.
   b) Select the **Password required** check box.
   c) Click **Test Connection** to test the connection.

      The **Authentication Password** dialog box displays.
   d) Enter the database password in the **Password** field, and click **OK**.
   e) Click **OK** on the **Connection Test** dialog box.

      For 64-bit Linux systems, if an error message (cannot open library) displays, complete the following steps.
      1. Issue the following command: **export LD_LIBRARY_PATH=/opt/PostgreSQL/8.4/lib/:/usr/lib64/:/opt/PostgreSQL/psqlODBC/lib/:$LD_LIBRARY_PATH**.
      2. Navigate to the Postgres ODBC library (default location is opt/PostgreSQL/psqlODBC/lib/).
      3. Create a list of missing libraries by issuing the following command: **ldd psqlodbcw.so**. Missing files display as: `libodbc.so.1=> not found`
      4. Find shared libraries with the same name as the missing library by issuing the following command: **find -name libodbc.so***
      5. Create a soft link for libodbc.so.1 pointing to libodbc.so.2.0.0 by issuing the following command: **ln -s libodbc.so.1 libodbc.so.2.0.0**.
   f) Click **Next**.
6. On the **Save and proceed** window, click **Finish**.

Smart card driver installation

Windows operating systems do not require smart card drivers to be installed separately; the driver is bundled with the operating system. However, you must install a smart card driver for Linux operating systems. You must install both the special USB Chip/Smart Card Interface Device (USB CCID) and the PC/SC IFD driver. You can download the source code and compile it from one of the following websites:

- USB CCID (ccid-1.3.7.tar.bz2)

  Open Source URL: http://pcsclite.alioth.debian.org/ccid.html

- Muscle PC/SC IFD Driver (pcsc-lite-1.4.101.tar.gz)

  Open Source URL: https://alioth.debian.org/frs/?group id=30105

The Encryption Manager Client within Management application provides the binary code on both platforms for installation. You must uncompress or untar the file depending on the platform. The thirdparty/pscs-lite-1.4.101-linux-x86.tar.gz file can be found on the Management application DVD.

Installing the smart card driver on the local client

1. Verify that the /opt directory exists.

   If the /opt directory does not exist, create an /opt directory. If you want to install the driver in a different directory, create that directory. Otherwise, skip this step.

   ```
   > su
   > mkdir /opt
   ```

2. Copy the appropriate pscs file for your platform (Linux) from the DVD, and rename the file as the pcsc-lite-1.4.101-linux-x86.tar.gz file.
3. Log in as superuser to untar the pcsc-lite-1.4.101-linux-x86.tar.gz file.

   ```
   > su
   > cd /opt
   > gunzip pcsc-lite-1.4.101-linux-x86.tar.gz
   > tar -xvf pcsc-lite-1.4.101-linux-x86.tar
   ```

   After the pcsc-lite-1.4.101.tar file is extracted, the necessary binary, library, and smart card drivers are stored in the /opt/pcsc directory.

4. If you installed a pcsc directory into a location other than /opt, modify the pcscctl script to change "/opt" to the directory.

   ```
   > cd <new_dir>
   > vi pcscctl
   ```

   Search for "/opt" and change it to the name of the new directory.

5. Create a soft link into the system directory to support the automatic restart of the pcscd daemon upon system restart.

   If you installed the pcsc directory into the /opt directory, just create the soft link. Otherwise, use the name of the new directory in place of /opt.

   ```
   S.u.s.e> ln -s /opt/pcsc/pcscctl /etc/init.d/pcscd
   S.u.s.e> chkconfig --add pcscd
   ```

   or

   ```
   redhat> ln -s /opt/pcsc/pcscctl /etc/init.d/pcscd
   redhat> chkconfig --add pcscd
   ```

   NOTE

   Before you enter **chkconfig --add pcscd**, you can enter **chkconfig -list | grep pcscd** to verify that the pcscd file is already on the list. If it already exists, you do not need to enter **chkconfig -add pcscd**. After you reboot the system, you should expect the following links under /etc/rc2.d, /etc/rc3.d, /etc/rc3.d, /etc/rc4.d, and /etc/rc5.d.

   ```
   lrwxrwxrwx 1 root root 15 Jul 28 01:50  S94pcscd -> ../init.d/pcscd
   ```

   NOTE

   For some Linux vendors, the smart card driver may come with the operating system. In this case, extra system configuration may be needed. For more information, refer to Detecting and correcting a default Linux smart card driver on page 46.

6. Start or stop the pcscd daemon.

   To start pcscd, type:

   ```
   > /opt/pcsc/pcscctl start
   ```

   To stop pcscd, type:

   ```
   > /opt/pcsc/pcscctl stop
   ```

Installing the smart card driver on the remote client

1. Complete steps 1 through 4 in Installing the smart card driver on the local client on page 44.

2. Run the following commands to support remote clients (Web Start).

```
> cd /usr/lib
> ln -s /opt/pcsc/lib/libpcsclite.so .
```

NOTE

If a soft link exists on libpcsclite.so, make sure that the final file is linked to /opt/pcsc/lib/libpcsclite.so.xxx. It is recommended that you back up the original.

```
> ls -l  libpcsc*
            lrwxrwxrwx 1 root root    20 Aug  4 16:16 libpcsclite.so ->
            libpcsclite.so.1.0.0
            lrwxrwxrwx 1 root root    20 Jun  4 12:30 libpcsclite.so.1 ->
            libpcsclite.so.1.0.0
            lrwxrwxrwx 1 root root    34 Aug  5 14:36 libpcsclite.so.1.0.0
> mv libpcsclite.so.1.0.0 libpcsclite.so.1.0.0.org
> ln -s /opt/pcsc/lib/libpcsclite.so.1.0.0   libpcsclite.so.1.0.0
> ls -l  libpcsc*
            lrwxrwxrwx 1 root root    20 Aug  4 16:16 libpcsclite.so ->
            libpcsclite.so.1.0.0
            lrwxrwxrwx 1 root root    20 Jun  4 12:30 libpcsclite.so.1 ->
            libpcsclite.so.1.0.0
            lrwxrwxrwx 1 root root    34 Aug  5 14:36 libpcsclite.so.1.0.0 ->
            /opt/pcsc/lib/libpcsclite.so.1.0.0
            -rwxr-xr-x 1 root root 35428 Aug  4 16:17 libpcsclite.so.1.0.0.org
```

Detecting and correcting a default Linux smart card driver

NOTE

The steps to detect and correct a default Linux smart card driver apply to the Linux system only. Some Linux systems may provide a default smart card driver and have their own setup to activate it. In this case, you must use the driver provided with Management application. Otherwise, an incompatibility issue between the driver and the native library could cause a driver detection failure. Complete the following steps to discover whether a default driver already exists and how to reconfigure the driver environment.

1. Detect a different smart card driver by running the following commands.

```
> cd /
> find . -name pcscd -print
```

If the results contain "pcscd", and it is not located under /opt/pcsc or /etc/init.d/pcscd, a different driver exists on the system.

2. Make sure that the pcscd file in the /etc/init.d directory is linked to /opt/pcsc/pcscctl by running the following commands.

```
> cd /etc/init.d
> ls -l pcscd
            lrwxrwxrwx 1 root root 17 Jul 28 01:29 pcscd -> /opt/pcsc/pcscctl
```

3. If there is an existing pcscd script in this directory, you can move and rename this file before you overwrite it.

```
> mv  /etc/init.d/pcscd   /etc/init.d/pcscd.org
```

4. Create a soft link using the following command.

```
> ln -s /opt/pcsc/pcscctl /etc/init.d/pcscd
```

The existing pcscd.org script in this directory implies that a different driver version exists. You can compare the existing one with the one under /opt/pcsc/pcscd/sbin. If the size is different and the existing pcscd script contains the following information, you must clean up the driver configuration. The following example shows a different pscsd.org script and how to cleanup the configuration. The configuration level is 2345, the start priority is 25, and the stop priority is 88.

```
> more /etc/init.d/pcscd
            #!/bin/sh
            #
            # pcscd        Starts the pcscd Daemon
            #
            # chkconfig:   2345   25  88
```

5. Remove the existing pcscd start priority file by deleting the file as *SNN*pcscd, where *NN* is the start priority. For example, from the preceding step, the file name is S25pcscd.

```
> find  /etc/.   -name "S25pcscd" -exec rm {} \; -print
> sync;sync;sync
> reboot
```

After the reboot, the new configuration from the /opt/pcsc/pcscctl file should be under the /etc/rc2.d, /etc/rc3.d, /etc/rc4.d, and /etc/rc5.d directories.

```
lrwxrwxrwx 1 root root 15 Jul 28 01:50 S94pcscd -> ../init.d/pcscd
```

6. For the remote client, ensure that the smart card native library is linked to the one under /opt/pcsc/lib.

```
> cd /
> find . -name libpcsclite.so* -print
```

If the library libpcsclite.so* exists in multiple locations, you must ensure that there is only one library under /lib or /usr/lib and that it is linked to the library in /opt/pcsc/lib correctly. For example, to find a copy of the library in /lib, use the following commands.

```
> cd /lib
> ls -al libpcsclite.so
```

If a copy of the library exists, either remove it or save it as a backup.

To find a copy of the library in /usr/lib, use the following commands.

```
> cd /usr/lib
> ls -al libpcsclite.so
```

Use this command for the soft link.

```
> ln -s  /opt/pcsc/lib/libpcsclite.so  /usr/lib/.
```

Configuring an explicit server IP address

If you selected a specific IP address from the **Server IP Configuration** window during installation and the selected IP address changes, you will not be able to connect to the server. To connect to the new IP address, you must manually update the IP address information.

To change the IP address, complete the following steps.

1. Choose one of the following options:
   - On Windows systems, select **Start** > **Programs** > **IBM Network Advisor 14.4.2** > **IBM Network Advisor Configuration**.
   - On UNIX systems, use the **sh** *Install_Home* **/bin/configwizard** command from the terminal.
2. Click **Next** on the **Welcome** window.
3. Click **Yes** on the confirmation message.
4. Click **Next** on the **FTP Server** window.
5. Complete the following steps on the **Server IP Configuration** window.
   a) Select an address from the **Server IP Configuration** list.

      NOTE
      The host name does not display in the list if it contains invalid characters. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default.

      If DNS is not configured for your network, do not select the "hostname" option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the "hostname" option prevents clients and devices from communicating with the server.

   b) Select an address from the **Switch - Server IP Configuration Preferred Address** list. The preferred IP address is used for switch and server communication.

      or

      Select **Any** from the **Switch - Server IP Configuration Preferred Address** list to enable switch and server communication with one of the reachable IP addresses present in the server. By default, the **Any** option is selected.

   c) Click **Next**.
6. Click **Next** on the **Server Configuration** window.
7. (SAN with SMI Agent) Click **Next** on the **SMI Agent Configuration** window.
8. (SAN with SMI Agent or SAN with SMI Agent + IP packages) Click **Next** on the **SMI Agent Configuration** screen.

   NOTE
   Beginning with version 14.4.0 release, the SAN with SMI Agent + IP package is not available for the new installation. It is available only for the migration from the earlier SAN+IP version.

9. Verify your server name on the **Server Configuration Summary** window and click **Next**.
10. Click **Finish** on the **Start Server** window.
11. Click **Yes** on the restart server confirmation message.
12. Enter your user name and password, and click **Login**.

    The defaults are Administrator and password.

    NOTE
    Do not enter Domain*User_Name* in the **User ID** field for LDAP server authentication.

13. Click **OK** on the login banner.

Configuring remote client access to the database

1. Open the pg_hba.conf file (in the Install_Home\data\databases\ directory).
2. To allow all IPv4 remote connections for all users, search for the following text and uncomment the second line:

```
# IPv4 remote connections (Uncomment below line to allow all IPv4 remote users):
#host    all             all             0.0.0.0/0               md5
```

3. To allow all IPv6 remote connections for all users, search for the following text and uncomment the second line:

```
# IPv6 remote connections (Uncomment below line to allow all IPv6 remote users):
#host    all             all             ::0/0                   md5
```

4. To allow access to a specific IPv4 address, search for the following text and uncomment the second line:

```
# Uncomment below line and provide IPV4 address to allow specific IPv4 remote user
#host    all             all             <IPV4 address>/32       md5
```

5. To allow access to a specific IPv6 address, search for the following text and uncomment the second line:

```
# Uncomment below line and provide IPV6 address to allow specific IPv6 remote user
#host    all             all             <IPV6 address>/128      md5
```

6. Save and close the file.

Data Migration

Upgrading the license

The quickest and simplest method of moving from one package to another is to enter the new license information on the **Management application License** dialog box. The following table lists the available upgrade paths.

TABLE 8 SAN upgrade paths

Current software release	To software release
SAN Professional	SAN Professional Plus or Licensed version SAN Enterprise Trial or Licensed version
SAN Professional Plus Licensed version	SAN Enterprise Licensed version
SAN Enterprise Trial	SAN Enterprise Licensed version

1. Select **Help** > **License**.

   The **Management application License** dialog box displays.
2. Browse to the license file (.xml), and click **Update**.
3. Click **OK** on the **Management application License** dialog box.
4. Click **OK** on the message.

   The client closes after updating the license successfully. Restart the server from the Server Management Console for the changes to take effect.
5. Open the application (double-click the desktop icon or open from the **Start** menu).

   The **Log In** dialog box displays.
6. Enter your user name and password.

   The defaults are Administrator and password. If you migrated from a previous release, your user name and password do not change.

   NOTE
   Do not enter Domain*User_Name* in the **User ID** field for LDAP server authentication.
7. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
8. Click **Login**.
9. Click **OK** on the Management application login banner.

Supported migration paths

NOTE
To migrate Enterprise and Professional Plus editions to a 64-bit server, refer to Premigration requirements on page 57.

NOTE
Management application 14.2.X includes 14.2.0 and 14.2.1.

NOTE
Management application 14.3.X includes 14.3.0 and 14.3.1.

NOTE
Management application 14.4.X includes 14.4.0, 14.4.1, and 14.4.2.

The following table shows the migration paths from DCFM.

TABLE 9 DCFM release migration path

DCFM starting version	Network Advisor 14.4.2
DCFM 10.4.X	DCFM 10.4.X > Network Advisor 11.1.X > Network Advisor 12.0.X > Network Advisor 12.3.X Network Advisor 12.4.X Network Advisor 14.0.X Network Advisor 14.2.X Network Advisor 14.3.X Network Advisor 14.4.1

The following table shows the migration paths from Network Advisor 12.1.X or earlier releases. Direct migration is not supported on pre-12.3.X releases.

TABLE 10 12.1.X and earlier release migration path

Current version	Network Advisor 14.4.2
Network Advisor 11.0.X	Network Advisor 11.0.X Network Advisor 11.1.X Network Advisor 12.0.X Network Advisor 12.3.X Network Advisor 12.4.X Network Advisor 14.0.X Network Advisor 14.2.X Network Advisor 14.3.X Network Advisor 14.4.2
Network Advisor 11.1.X	Network Advisor 11.1.X Network Advisor 12.0.X Network Advisor 12.3.X

TABLE 10 12.1.X and earlier release migration path (continued)

Current version	Network Advisor 14.4.2
	Network Advisor 12.4.X
	Network Advisor 14.0.X
	Network Advisor 14.2.X
	Network Advisor 14.3.X
	Network Advisor 14.4.2
Network Advisor 11.2.X	Network Advisor 11.2.X
	Network Advisor 12.0.X
	Network Advisor 12.3.X
	Network Advisor 12.4.X
	Network Advisor 14.0.X
	Network Advisor 14.2.X
	Network Advisor 14.3.X
	Network Advisor 14.4.2
Network Advisor 11.3.X	Network Advisor 11.3.X
	Network Advisor 12.0.X
	network Advisor 12.1.X
	Network Advisor 12.3.X
	Network Advisor 12.4.X
	Network Advisor 14.0.X
	Network Advisor 14.2.X
	Network Advisor 14.3.X
	Network Advisor 14.4.2
Network Advisor 12.0.X	Network Advisor 12.0.X
	Network Advisor 12.1.X
	Network Advisor 12.3.X
	Network Advisor 12.4.X
	Network Advisor 14.0.X
	Network Advisor 14.2.X
	Network Advisor 14.3.X
	Network Advisor 14.4.2
Network Advisor 12.1.X	Network Advisor 12.1.X
	Network Advisor 12.3.X
	Network Advisor 12.4.X
	Network Advisor 14.0.X
	Network Advisor 14.2.X
	Network Advisor 14.3.X
	Network Advisor 14.4.2

The following table shows the direct migration paths from the Network Advisor 14.0.0 or later Professional, Trial, and Licensed versions. For the step-by-step migration procedure, refer to Migrating data on page 61.

NOTE
Data migration is not supported from 12.4.4 to 14.0.0.

TABLE 11 Network Advisor version migration paths

Current version	Professional version	Trial version	Licensed version		
			Enterprise	Professional Plus	Enterprise
Network Advisor 14.0.X Professional[12]	Yes	Yes	Yes	Yes	
Network Advisor 14.0.X Professional Plus Licensed[12]	No	No	Yes	Yes	
Network Advisor 14.0.X Enterprise Trial[12]	No	Yes	No	Yes	
Network Advisor 14.0.X Enterprise Licensed[12]	No	Yes	No	Yes	
Network Advisor 14.1.X Professional	Yes	Yes	Yes	Yes	
Network Advisor 14.1.X Professional Plus Licensed	No	No	Yes	Yes	
Network Advisor 14.1.X Enterprise Trial	No	Yes	No	Yes	

[12] Network path migration and migration from partially uninstalled data are not supported due to the upgrade of major postgress version from 9.2.9 to 9.4.4.

TABLE 11 Network Advisor version migration paths (continued)

Current version	Professional version	Trial version	Licensed version		
			Enterprise	Professional Plus	Enterprise
Network Advisor 14.1.X Enterprise Licensed	No	Yes	No	Yes	
Network Advisor 14.2.X Professional	Yes	Yes	Yes	Yes	
Network Advisor 14.2.X Professional Plus Licensed	No	No	Yes	Yes	
Network Advisor 14.2.X Enterprise Trial	No	Yes	No	Yes	
Network Advisor 14.2.X Enterprise Licensed	No	Yes	No	Yes	
Network Advisor 14.3.X Professional	Yes	Yes	Yes	Yes	
Network Advisor 14.3.X Professional Plus Licensed	No	No	Yes	Yes	
Network Advisor 14.3.X Enterprise Trial	No	Yes	No	Yes	
Network Advisor 14.3.X Enterprise Licensed	No	Yes	No	Yes	
Network Advisor 14.4.X Professional	Yes	Yes	Yes	Yes	
Network Advisor 14.4.X Professional Plus Licensed	No	No	Yes	Yes	

TABLE 11 Network Advisor version migration paths (continued)

Current version	Professional version	Trial version	Licensed version		
			Enterprise	Professional Plus	Enterprise
Network Advisor 14.4.X Enterprise Trial	No	Yes	No	Yes	
Network Advisor 14.4.X Enterprise Licensed	No	Yes	No	Yes	

The following table shows the migration paths from SMI Agent only. For the step-by-step migration procedures, refer to Migrating data on page 61.

TABLE 12 SMI Agent only migration paths

Current version	Professional version	Enterprise Trial version	Licensed version	SMI Agent only	
			Professional Plus		Enterprise
Network Advisor 14.4.2 SMI Agent only	No	No	No	No	Yes

DCFM migration paths

NOTE

Before you migrate from DCFM to Network Advisor 11.0.X, 11.1.0, 11.1.1, or 11.1.2, you must reset your DCFM password back to the default (password).

You cannot migrate directly from DCFM 10.0.X, DCFM 10.1.X, or DCFM 10.3.X to Network Advisor 14.4.2. You must first migrate to DCFM 10.4.X, then to Network Advisor 11.1.X, then to Network Advisor 12.0.X, then to Network Advisor 12.2.X, then to Network Advisor 12.3.X, then to Network Advisor 12.4.X, then to Network Advisor 14.0.X, and then to Network Advisor 14.4.2.

To migrate from DCFM 10.0.X, DCFM 10.1.X, or DCFM 10.3.X to DCFM 10.4.X, contact your customer representative. To migrate from DCFM 10.4.X to Network Advisor 11.1.X, refer to the Network Advisor migration guide for Network Advisor 11.1.X.

Premigration requirements

Before you install Management application, make sure that you meet the following premigration requirements.

- Make sure that all system requirements have been met before to installation.
- Check for and install the latest Java patches for your operating system. For the current supported JRE version for Management application and Web Tools, refer to the release notes. For the website listing patch information, go to http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- Make sure that you fully back up your current Management application data on your Management server.
- Make sure that you close all instances of the application before migrating.
- Make sure to install Management application on the same system as your current Management application.
- Make sure that minimum free space is 1.5 times the size of the Management application data folder (<Install_Home>\data) available for performing migration for servers with a large amount of Performance, Events, and Flow Vision data in the database.
- If you are migrating within the same release or you are migrating from Professional to Licensed software, make sure to partially uninstall the application.
- Partial data migration is not supported from pre-12.0.0 releases. If you are migrating data from a partially uninstalled source, complete the following steps:
    1. Re-install your current Management application version on the same machine, and migrate the partially uninstalled data. If your current release is pre-11.3.X, you must migrate to Management application 11.3.0 or later.
    2. Install Management application 12.1 on the same machine, and migrate your data.
- Make sure that minimum free space is 1.5 times the size of the Management application data folder (<Install_Home>\data) available for performing migration for servers with a large amount of Performance, Events, and Flow Vision data in the database.

Premigration requirements when migrating from one server to another

If you are migrating from Management application 14.2.X on a 64-bit Windows server1 to Management application 14.4.2 on a 64-bit Windows server2, complete the following steps.

1. Back up the server for 14.2.X using **Options > Server Backup** on the 64-bit Windows server1.
2. Install Management application 14.2.X on the 64-bit Windows server2.
3. Select the **SMC > Restore** tab to restore the backup on the 64-bit Windows server1.
4. Install Management application 14.4.2 on the 64-bit Windows server2.

   Perform a seamless migration to Management application 14.4.2 (refer to Data Migration on page 51).

If you are migrating from Management application 14.2.X on a 64-bit Linux server1 to Management application 14.4.2 on a 64-bit Linux server2, complete the following steps.

1. Install and migrate to Management application 14.4.2 in the same machine (refer to Supported migration paths on page 52).
2. Back up the server using **Options > Server Backup** on the 64-bit Linux server.
3. Install Management application 14.4.2 on the 64-bit Linux server2.
4. Select the **SMC > Restore** tab to restore the backup on the 64-bit Linux server1.

If you are migrating from a pre-14.0.X release on a 64-bit Windows server1 to Management application 14.4.2 on a 64-bit Windows server2, complete the following steps.

1. Install and migrate to Management application 14.4.2 in the same machine (refer to Supported migration paths on page 52).
2. Back up the server using **Options > Server Backup** on the 64-bit Windows server.
3. Install the same version (14.4.2) on the 64-bit Windows server1.
4. Select the **SMC > Restore** tab to restore the backup on the 64-bit Windows server.

If you are migrating from Management application 14.4.2 on a 64-bit Windows server1 to Management application 14.4.2 on a 64-bit pure Windows server2, complete the following steps.

1. Back up the server for Management application 14.4.2 using **Options > Server Backup** on the 64-bit Windows server1.
2. Install Management application 14.4.2 on the 64-bit pure Windows server2.
3. Select the **SMC > Restore** tab to restore the backup on the 64-bit Windows server1.

If you are migrating from Management application 14.4.2 on a 64-bit Linux server1 to Management application 14.4.2 on a 64-bit pure Linux server2, complete the following steps.

1. Back up the server for 14.4.2 using **Options > Server Backup** on the 64-bit Linux server1.
2. Install the same version (14.4.2) on the 64-bit pure Linux server2.
3. Select the **SMC > Restore** tab to restore the backup on the 64-bit Linux server1.

If you are migrating from a pre-14.2.X release on a 64-bit Linux server1 to Management application 14.4.2 on a 64-bit pure Linux server2, complete the following steps.

1. Install and migrate to Management application 14.4.2 in the 64-bit Linux server1 (refer to Supported migration paths on page 52).
2. Back up the server using **Options > Server Backup** on the 64-bit Linux server1.
3. Install the same version (14.4.2) on the 64-bit pure Linux server2.
4. Select the **SMC > Restore** tab to restore the backup on the 64-bit Linux server1.

If you are migrating from a Windows server that is no longer supported to a supported Windows server, complete the following steps. For a list of supported operating system servers, refer to Table 2 on page 11 table.

NOTE
If you are migrating from a pre-12.4.X release, you must first migrate to Management application 14.2.X on your current server for the release migration path.

1. Install Management application 14.2.X on your current machine (refer to Installation on page 11), and migrate your data (Migrating data on page 61).

2. Install Management application 14.4.2 on your new machine (refer to Data Migration on page 51), and migrate your data (Migrating data on page 61).

Cross OS migration is not supported; however, you can restore a Windows OS backup to Linux OS and vice versa. If you are migrating from one OS to another, complete the following steps:

1. Back up the server for 14.4.2 using **Options > Server Backup** on the 64-bit Windows server1.
2. Install the same version (14.4.2) on the 64-bit pure Linux server2.
3. Select the **SMC > Restore** tab to restore the backup on the 64-bit Windows server1.

Additional premigration requirements on UNIX systems

- Make sure that the current application services are running.
  1. Go to *Install_Home*/bin.
  2. Issue . **/smc** or **sh smc**.
  3. Click the **Services** tab. The tab lists the Management application services.
  4. Click **Start**, if necessary.
- Make sure that an X Server is available for display and is configured to permit X Client applications to display from the host on which they are installing the Management application server (typically, this simply requires that the systems console be present and running with a logged-in user on the X Server-based desktop session, such as KDE, and GNOME).
- Make sure that the DISPLAY environment variable is correctly defined in the shell with a valid value (for example, to display to the local console, **export DISPLAY=:0.0**, or to display to a remote system that has an X Server running, **export DISPLAY=***Remote_IP_Address***:0.0**).

  NOTE
  You may also need to consider a firewall, which may block the display to the X Server, which listens by default on TCP port 6000 on the remote host. To display to a remote system, you must permit the remote display of the X Server by running the **xhost +IP** command, where IP is the IP address of the Management application server host from the X-based desktop of the remote system.

- Make sure that you test the DISPLAY definition by running the **xterm** command from the same shell from which you ran install.bin. A new X terminal window to the destination X Server opens.

Additional trial requirements

- Three versions of the Management application cannot reside on the same host unless there are two guest operating systems on the host.
- Data collected during the trial cannot be migrated back to the Professional software.
- Once the Enterprise trial period expires, you must upgrade to Licensed software.

Data migration for Management application

While performing a data migration, you must understand the following information.

> NOTE
> Network Advisor 14.4.0 supports migration only from earlier IP releases. Migration from the SAN or SAN+IP package is not supported.

Some upgrade options are not supported:

- Migration from Trial to Professional software is not supported.
- Migration from Licensed software to Trial software is not supported.
- Migration from Enterprise software to Professional Plus software is not supported.

During data migration, Management application and SMIA certificates will migrate from the source to the destination according to the following requirements. If none of the requirements is followed, a new certificate will be generated using the SHA-256 signature algorithm.

- Certificates must be generated by customers.
- Certificates must have the SHA-2 signature algorithm.
- The source certificate must be self-signed and have a validity of more than six months or be generated using the SHA-256 signature algorithm.

Ensure that you have configured the Brocade E-mail Call Home center. For details, refer to a Brocade Network Advisor User Manual or to online help.

> NOTE
> You must be running the Enterprise edition for the following devices:
>
> - SAN768B
> - SAN768B-2
> - SAN256B-6
> - SAN512B-6

Management server or client issues

If the Management server has multiple network interface cards and if any interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:

- Configuration wizard (does not display all IP addresses)
- Trap and Syslog autoregistration
- Report content (Ipconfiguration element does not display all server IP addresses)
- Network OS configuration backup through FTP
- Network OS configuration backup through FTP
- Trace dump through FTP

If the Management client has multiple network interface cards and if any interfaces are not plugged in, you must disable them; otherwise, the following features do not work properly:

- Options dialog box (does not display all IP addresses)
- Firmware import and download dialog box

- Firmware import for Network OS products
- Firmware import for Fabric OS products
- Firmware import for Fabric OS and Network OS products
- FTP button in the Technical Support Repository dialog box
- Technical supportSave of Network OS and host products through FTP
- Technical supportSave of Fabric OS and host products through FTP
- Technical supportSave of Fabric OS, Network OS, and host products through FTP

Migrating data

While upgrading from one version of Management application to another version, the data must be migrated.

You must enter the new license information before migrating the data. Refer to Upgrading the license on page 51.

Beginning with version 14.4.2 release, the following migration support applies:

Source package	Migration support to 14.4.2
SAN only	Yes

NOTE
If an error occurs while migrating from Management application 14.2.X or earlier to Management application 14.4.2, the current release version rolls back to the earlier version. Migration rollback is not supported if you are performing headless migration.

NOTE
Management application 14.4.2 supports migration only from earlier SAN or SAN + IP releases. Migration from the IP only package is not supported.

NOTE
When you migrate from a pre-14.1.X release to Management application 14.4.2, Management application will remove the flows and statistics retrieved from the Brocade Analytics Monitoring Platform pre-14.1.X release and the AMP-specific dashboards **SAN Analytics Monitoring-Top Flows** and **SAN Analytics Monitoring-Summary** post the migration.

Migrating data from a previous version, may take several minutes after you click **Start** on the **Data Migration** window.

1. Click **Next** on the **Welcome** window.
2. Choose one of the following options:
   - If data is detected on your system, the **Copy Data and Settings from previous releases** window displays. To migrate data from the previous version installed (automatically detected), select **Yes, from the following location**. Continue to step 4.
   - If data is not detected, the **Copy Data and Settings from previous releases** window displays. Continue to step 3.
3. Choose one of the following options:
   a) Select **Yes, from this machine or on network**, and click **Browse** to browse to the installation directory.
   b) Click **Next** on the **Copy Data and Settings from previous releases** window.

   If you are migrating to the same installation location (as the previous version), you will need to browse to the renamed directory on the **Copy Data and Settings from previous releases** window.
4. Click **Start** on the **Data Migration** window.

   Data migration may take several minutes. When data migration is complete, the previous version is partially uninstalled.

5. Click **Next** on the **Data Migration** window.

   If you have products associated with the Brocade North America or Brocade International Call Home centers, a message displays. To map these Call Home centers to the Brocade E-mail Call Home center after migration, click **Yes**. To not map these Call Home centers, click **No**.

6. Select one of the following options on the **Installation Type** window and click **Next**:

   NOTE
   SAN768B, SAN768B-2, SAN256B-6, and SAN512B-6 Chassis require the Enterprise edition.

   - **Management application - Licensed version**: If you choose the Licensed version, you must enter a license key during configuration to enable features and configuration.
   - **Management application - 120 days Trial**: If you choose the Trial version, once the trial period ends (120 days), you must upgrade to Licensed software. The trial version enables you to manage your networks from a single interface for 120 days.
   - **Management application - Professional**: The Professional version is bundled with Fabric OS devices to manage small networks from a single interface.

7. Choose one of the following options on the **Server License** window:

   - If you are migrating from a licensed source, the source license information displays. Click **Next**.
   - If you are migrating from Professional or Trial software to Licensed software, browse to the license file (.xml), and click **Next**.

   The **License Key** field is not case-sensitive. Downgrading the license from the current configuration during migration is not supported.

8. Complete the following steps on the **FTP/SCP/SFTP Server** window. The default selection reflects the previous edition configuration.
   a) Choose one of the following options:
      - Select **Built-in FTP/SCP/SFTP Server** to configure an internal FTP, SCP, or SFTP server, and select one of the following options:
        - Select **Built-in FTP Server** to configure an internal FTP server. The internal FTP server uses a default account and port 21. You can configure your own account from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor user manual or to online help.
        - Select **Built-in SCP or SFTP Server** to configure an internal SCP or SFTP server. The internal SCP or SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor user manual or to online help.
      - Select **External FTP, SCP, or SFTP Server** to configure an external FTP server. You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to a Brocade Network Advisor user manual or to online help.
   b) Click **Next**.

      If port 21 or 22 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured, make sure that port 21 or 22 is free, and restart the server to start the FTP, SCP, or SFTP service.

      NOTE
      If you use an FTP/SCP/SFTP server that is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.

      NOTE
      If port 22 is occupied, the following details are the workaround for Linux,

      - To find all processes, issue the following command: `Kill -9 <PID>`.
      - If SCP and SFTP services are already running, issue the following command: `lsof -i tcp:22` and terminate the process with the same id running in both IPv4 and IPv6 in SSHD services.
      - If FTP services are already running, issue the following command: `lsof -i tcp:21` and terminate the process with the same id running in both IPv4 and IPv6 FTP services.
      - If Database services are already running, issue the following commands:

        ```
        lsof -i tcp:5432
        kill -9 <pidofthatprocess>
        ```

      For windows:

      - To find all processes running in FTP(21), SCP(22), and Database(5432), issue the following command: `netstat -aon` and terminate the process by issuing the following command: `taskkill /F /PID <processid>`.

9. Complete the following steps on the **Server IP Configuration** window.
   a) Select an address from the **Server IP Configuration** list.

      NOTE
      For Professional software, the **Server IP Configuration** address is set to "localhost" by default. You cannot change this address.

      NOTE
      For SMI Agent, if the **Server IP Configuration** list contains a duplicate IP address or is empty, an error message displays and the configuration wizard closes.

   b) Select an address from the **Switch - Server IP Configuration Preferred Address** list.

      NOTE
      If the "hostname" contains invalid characters, the host name does not display in the list. Valid characters include alphanumeric and dash (-) characters. The IP address is selected by default.

      If DNS is not configured for your network, do not select the "hostname" option from either the **Server IP Configuration** list or the **Switch - Server IP Configuration Preferred Address** list. Selecting the "hostname" option prevents clients and devices from communicating with the server.

      If you select a specific IP address from the **Server IP Configuration** window and the selected IP address changes, you will not be able to connect to the server. To change the IP address, refer to Configuring an explicit server IP address on page 47.

   c) Click **Next**.

10. Complete the following steps on the **Server Configuration** window.

    FIGURE 3 Server Configuration window

    a) Enter a port number in the **Web Server Port # (HTTPS)** field (default is 443).

    b) Enable HTTP redirection to HTTPS by selecting the **Redirect HTTP Requests to HTTPS** check box.

    When you enable HTTP redirection, the server uses port 80 to redirect HTTP requests to HTTPS. You can configure the server port settings from the **Options** dialog box (**Server Port** pane). For instructions, refer to a Brocade Network Advisor user manual or to online help.

    c) Enter a port number in the **Database Port #** field (default is 5432).

    NOTE
    Do not use a port number below 1024.

    d) Enter a port number in the **Starting Port #** field (default is 24600).

    NOTE
    The server requires 11 consecutive free ports beginning with the starting port number.

    e) Enter a port number in the **Syslog Port #** field (default is 514).

    NOTE
    If the default syslog port number is already in use, you will not receive any syslog messages from the device. To find and stop the process currently running on the default syslog port number.

    f) Enter a port number in the **SNMP Port #** field (default is 162).

    g) Enter a port number in the **TFTP Port #** field (default is 69).

    NOTE
    The **TFTP Port#** field is available only for SAN + IP package.

    h) Click **Next**.

    If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** window and edit the syslog port number. Click **Yes** to close the message.

    If you enter a port number already in use, a warning displays next to the associated port number field. Edit that port number, and click **Next**.

11. (SAN with SMI Agent) Complete the following steps on the **SMI Agent Configuration** window.

    a) Enable the SMI Agent by selecting the **Enable SMI Agent** check box.

    b) Enable SLP by selecting the **Enable SLP** check box, if necessary.

    SLP is enabled only after you select the **Enable SMI Agent** check box.

    c) Enable SSL by selecting the **Enable SSL** check box, if necessary.

    SSL is enabled only after you select the **Enable SMI Agent** check box.

    d) Enter the SMI Agent port number in the **SMI Agent Port #** field (the default is 5989 if **SSL Enabled** is selected; otherwise, the default is 5988).

    e) Click **Next**.

12. (SAN with AMP Management) Complete the following steps on the **AMP Management** window.

    FIGURE 4 AMP Management

    a) Enable the AMP by selecting the **Enable AMP Management** check box.

    The **Database Port#** and **Web Server Port# (HTTPS)** fields display the default port numbers.

    The default port number for the **Database Port#** field is **5433** and for the **Web Server Port# (HTTPS)** field is **8443**.

    b) Click **Next**.

13. (SAN Enterprise or SMI Agent) Select one of the following options on the **SAN Network Size** window, and click **Next**:
    - **Small (managing up to 2000 switch ports, 1-20 domains)**
    - **Medium (managing up to 5000 switch ports, 21-60 domains)**
    - **Large (managing up to 15000 switch ports, 61-120 domains)**

    The port count is equal to the total number of switch ports across all fabrics.

14. Enable feature usage data transfer from the application by selecting the **Yes, I want to participate** option.

    You can stop participating at any time. To view an example of the usage data, click **View Example Data**. To stop participating in feature usage data transfer after configuration.

15. Verify your configuration information on the **Server Configuration Summary** window, and click **Next**.
16. Complete the following steps on the **Start Server** window:
    a) (Trial and Licensed only) Select the **Start SMI Agent** check box, if necessary.
    b) (Trial and Licensed only) Select the **Start SLP** check box, if necessary.
    c) Select the **Start Client** check box, if necessary.
    d) Click **Finish**.

    After all services are started, the **Log In** dialog box displays.

    To make changes to the configuration, you can re-launch the configuration wizard (refer to Configuring an explicit server IP address on page 47).

17. Enter your user name and password.

    The defaults are Administrator and password. If you migrated from a previous release, your user name and password do not change.

    NOTE
    Do not enter Domain*User_Name* in the **User ID** field for LDAP server authentication.

18. Click **Login**.
19. Click **OK** on the Management application login banner.

Cross flavor migration

To migrate from Management application 14.0.X/14.1.X to a Non-Management application 14.4.2 complete the following steps:

1. Install Management application 14.0.X/14.1.X/14.2.X/14.3.X (refer to Installing the application on page 20).
2. Install Non-Management application 14.4.2 (refer to Installing the application on page 20).

3. Migrate the supported (partial or full) data from Management application 14.4.2 (refer to Migrating data on page 61) to Non-Management application 14.4.1 by browsing to the Management application 14.4.1 location on the **Copy Data and Setting** window.

   NOTE
   If the Non-Management application does not support SAN + IP, it is recommended to install the SAN only Management application and then migrate to the Non-Management application.

Migration rollback

Migration rollback is triggered when a failure occurs while migrating to a different version of Management application. After successful rollback, the previous version will be running and the destination version will be uninstalled. The destination version failure logs and the source version supportSave will be zipped and stored at the source BNA_HOME\support folder in the following . zip file format:

```
Zip file format, Migration_Failure_SupportSave_<Time stamp>.zip
```

Migration rollback due to insufficient space

When migration rollback fails due to insufficient space, you can either increase the disk space and try rollback or cancel the migration rollback. The destination version is uninstalled manually if you cancel the migration rollback. Use the following commands to retrieve the source version.

- For Windows:

  ```
  Install_Home >bin>dbsvc install
  Install_Home >bin>dbsvc start
  Install_Home >bin>service.bat dcmsvc install
  Install_Home >bin>service.bat dcmsvc start
  ```

- For Windows, if SLP is enabled:

  ```
  Install_Home >cimom>bin>slpd.bat -install
  Install_Home >cimom>bin>slpd.bat -start
  ```

- For Windows, if CIMOM is enabled:

  ```
  Install_Home >bin>service.bat cimomsvc install
  Install_Home >bin>service.bat cimom svc start
  ```

- For Linux:

  ```
  Install_Home >bin>sh dbsvc start
  Install_Home >bin>sh service dcmsvc start
  ```

- For Linux, if SLP is enabled:

  ```
  Install_Home >bin>sh slpsvc start
  ```

- For Linux, if CIMOM is enabled:

  ```
  Install_Home >bin>sh service cimomsvc start
  ```

Migration rollback in configuration wizard

You can roll back to the earlier version of Management application during migration by canceling the configuration using the **Cancel** button.

You cannot cancel the migration while you are in the **Welcome** or **Copy and Data Setting** pages of the configuration wizard.

If you try to cancel the migration before it starts, the warning message "`Are you sure you want to cancel the configuration of Network Advisor 14.4.2`?" displays.

If you try to cancel the migration after it succeeds, the warning message "`Canceling the migration will initiate rollback of the changes made and will uninstall Network Advisor 14.4.2 Are you sure you want to continue`?" displays.

NOTE

The supportSave will not be triggered if you manually cancel the installation and initiate the rollback.

Click **Yes** to quit and close the configuration wizard.

Click **No** to stay on the same page.

Uninstallation

This chapter details uninstallation of the Management application and SMI Agent from both Windows and UNIX systems.

NOTE

Management application is installed in a separate directory from your previous version; therefore, you do not need to uninstall the previous version immediately. However, you cannot run both versions simultaneously.

Uninstalling from Windows systems

Complete the following steps to uninstall Management application and SMI Agent from your Windows system.

1. Select **Start** > **Programs** > **Management application 14.4.2** > **Uninstall Management application**.
2. Select one of the following options from the **Uninstall Option** window:
   - **Partial Uninstall**: Configuration and performance data is retained to be re-used by the new installation. This is the default option.
   - **Full Uninstall**: All data is removed.
3. Click **Uninstall**.
4. Click **Done** on the **Uninstall Complete** window.

Uninstalling from Windows systems (headless uninstall)

If the application was installed using headless installation, complete the following steps to uninstall Management application and SMI Agent from your Windows server.

1. Open a command prompt.
2. Choose one of the following options:
   - To partially uninstall Management application (configuration and performance data is retained to be re-used by the new installation), issue *Install_Home***Uninstall_Network Advisor 14.4.2****Uninstall_Network Advisor 14.4.2.exe -f** *<absolute path of partial uninstall property file>*.
   - To fully uninstall Management application (all data is removed), issue *Install_Home***Uninstall_Network Advisor 14.4.2****Uninstall_Network Advisor 14.4.2.exe -f** *<absolute path of full uninstall property file>*.

   When uninstallation is complete, an "Uninstallation complete" message displays. You must manually delete the *Install_Home*/silent folder.

Uninstalling from UNIX systems

Complete the following steps to uninstall Management application and SMI Agent from your UNIX system.

NOTE
The Uninstall folder is retained.

1. Go to *Install_Home*/Uninstall_Management application 14_4_2.
2. Execute **./Uninstall_Management application 14_4_2**.
3. Select one of the following options on the **Uninstall Option** window:
   - **Partial Uninstall**: Configuration and performance data is retained to be re-used by the new installation. This is the default option.
   - **Full Uninstall**: All data is removed.
4. Click **Uninstall**.
5. Click **Done** on the **Uninstall Complete** window.

Uninstalling from UNIX systems (headless uninstall)

If the application was installed using headless installation, complete the following steps to uninstall Management application and SMI Agent from your UNIX server.

1. Go to *Install_Home*/Uninstall_Network_Advisor14_4_2.
2. Choose one of the following options:
   - To partially uninstall Management application (configuration and performance data is retained to be re-used by the new installation), issue **Uninstall_Network_Advisor 14_4_2 -f***<absolute path of partial uninstall property file>*.
   - To fully uninstall Management application (all data is removed), issue **\Uninstall_Network_Advisor 14_4_2 -f** *<absolute path of full uninstall property file>*.

   When uninstallation is complete, an "Uninstallation complete" message displays. You must manually delete the *Install_Home*/silent folder.

References

Management application packages

The following table summarizes the packages and available editions for each package.

TABLE 13 Management application packages and versions

Package	Editions
SAN with SMI Agent	• Enterprise (Trial and Licensed) • Professional Plus (Licensed) • Professional
SMI Agent	NOTE Management application clients are not available in the SMI Agent only package. Clients are not required when other management tools are used in SMI Agent.

For a list of the supported scalability limits for the Management application by edition, refer to Scalability limits on page 71.

Scalability limits

The following table summarizes the scalability limits supported for Management application by edition.

TABLE 14 Supported scalability limits by Management application edition

	Enterprise edition			SAN Professional Plus edition	Professional edition
	Small	Medium	Large		
SAN switch ports	2000	5000	15,000	2560	300
SAN Switches and Access Gateways	40	100	400	40	15
SAN Devices	5000	15000	40,000	5000	1000
SAN Fabrics	25	50	100	36	2
Managed Hosts	20	100	400	100	20
vCenters	1	5	10	5	1
VMs (inlcudes powered-down VMs)	1000	5000	10,000	5000	1000
ESX Hosts	200	1000	2000	1000	200

NOTE

Virtual Fabrics are counted as fabrics when calculating the managed count limits.

NOTE
SMI Agent is not supported in the Professional edition.

NOTE
Supported network latency between the Management application server and client or between the server and devices is 100 milliseconds.

Management server and client ports

The Management application has two parts: the server and the client. The server is installed on one machine and stores device-related information; it does not have a user interface. To view information through a user interface, you must log in to the server through a client. The server and clients may reside on the same machine or on separate machines. If you are running Professional, the server and the client must be on the same machine.

In some cases, a network may utilize a virtual private network (VPN) or firewall technology, which can prohibit communication between products and the servers or clients. In other words, a server or client can find a product, appear to log in, but be immediately logged out because the product cannot reach the server or client. To resolve this issue, check to determine if the ports in the following table need to be opened up in the firewall.

NOTE
The Professional edition does not support remote clients.

The following table lists the default port numbers and whether the port needs to be opened up in the firewall, and it includes the following information:

- **Port number**: The port at the destination end of the communication path.
- **Ports**: The name of the port.
- **Transport**: The transport type (TCP or UDP).
- **Description**: A brief description of the port.
- **Communication path**: The "source" to "destination" values. Client and server refer to the Management application client and server unless stated otherwise. Product refers to the Fabric OS, Network OS, or IronWare OS devices.
- **Open in firewall**: Whether the port needs to be open in the firewall.

NOTE
For bidirectional protocols, you must open the firewall port bi-directionally.

TABLE 15 Port usage and firewall requirements

Port number	Ports	Transport	Description	Communication path	Open in firewall
20[13]	FTP port (control)	TCP	FTP control port for internal FTP server.	Client-Server Product-Server	Yes
21[13]	FTP port (data)	TCP	FTP data port for internal FTP server.	Client-Server Product-Server	Yes

[13] Port does not need to be open in the firewall for Professional edition.

TABLE 15 Port usage and firewall requirements (continued)

Port number	Ports	Transport	Description	Communication path	Open in firewall
22[14]	SSH, SCP, or SFTP	TCP	Secure Telnet and secure upload and download to product.	Server-Product Client-Product Product-Server	Yes
23	Telnet	TCP	Telnet port from server or client to product.	Server-Product Client-Product	Yes
25[14]	SMTP server port	TCP	SMTP server port for e-mail communication if you use e-mail notifications without SSL.	Server-SMTP Server	Yes
49[14]	TACACS+ authentication port	TCP	TACACS+ server port for authentication if you use TACACS+ as an external authentication.	Server-TACACS+ Server	Yes
69	TFTP	UDP	File upload/download to product.	Product-Server	Yes
80[14]	Management application HTTP server	TCP	Non-SSL HTTP/1.1 connector port if you use secure client-server communication. You need this port for HTTP redirection.	Client-Server	Yes
80[13]	Product HTTP server	TCP	Product non-SSL HTTP port for HTTP and CAL communication if you do not use secure communication to the product.	Server-Product	Yes
			Product non-SSL HTTP port for HTTP and CAL communication if you do not use secure communication to the product and you do not use the Management application server proxy.	Client-Product	Yes
161[14]	SNMP port	UDP	Default SNMP port.	Server-Product	Yes
162[14]	SNMP trap port	UDP	Default SNMP trap port.	Product-Server	Yes
389	LDAP authentication server port	UDP TCP	LDAP server port for authentication if you use LDAP as an external authentication.	Server-LDAP Server	Yes
443[13],[14]	HTTPS server	TCP	HTTPS (HTTP over SSL) server port if you use secure client-server communication.	Client-Server	Yes
443[14]			HTTPS (HTTP over SSL) server port if you use secure communication to the product.	Server-Product	Yes
443			HTTPS (HTTP over SSL) server port if you use secure communication to the product and you do not use the Management application server proxy.	Client-Product	Yes
443[14]			HTTPS (HTTP over SSL) server port if you use vCenter discovery.	Server-vCenter Server	Yes

[14] The default port number. You must use the same port number for all products or hosts managed by the Management server. This port is configurable in the Management server; however, some products and firmware versions do not allow you to configure a port.
[13] Port does not need to be open in the firewall for Professional edition.

TABLE 15 Port usage and firewall requirements (continued)

Port number	Ports	Transport	Description	Communication path	Open in firewall
465[14]	SMTP server port for SSL	TCP	SMTP server port for e-mail communication if you use e-mail notifications with SSL.	Server-SMTP Server	Yes
514[14]	Syslog port	UDP	Default syslog Port.	Product-Server Managed Host-Server	Yes
636[14]	LDAP authentication SSL port	TCP	LDAP server port for authentication if you use LDAP for external authentication and SSL is enabled.	Server-LDAP Server	Yes
1812[14]	RADIUS authentication server port	UDP	RADIUS server port for authentication if you use RADIUS for external authentication.	Server-RADIUS Server	Yes
1813[14]	RADIUS accounting server port	UDP	RADIUS server port for accounting if you use RADIUS for external authentication.	Server-RADIUS Server	Yes
5432	Database port	TCP	Port used by the database if you access the database remotely from a third-party application.	Remote ODBC-Database	Yes
5433	Database port	TCP	Port used by the AMP if you access the amp database remotely from a third-party application.	Remote ODBC-Database	Yes
5988	SMI server port	TCP	SMI server port on the Management application and the CIM/SMI port on HBAs if you use SMI Agent without SSL.	SMI Client-Server	Yes
				Server-Managed Host	Yes
5989[13,14]	SMI server port with SSL enabled	TCP	SMI Agent port on the Management application and the CIM/SMI port on HBAs if you use SMI Agent with SSL.	SMI Agent Server-Client	Yes
				Server-Managed Host	Yes
6343[14]	sFlow	UDP	Receives sFlow data from products if you are monitoring with sFlow.	Product-Server	Yes
8443	Web Server Port (HTTPS)	TCP	HTTPS (HTTP over SSL) server port if you use secure client-server communication.	Client-Server	Yes
			HTTPS (HTTP over SSL) server port if you use secure communication to the product.	Server-Product	Yes
24600[13,14]	JBoss remoting connector port	TCP	Use for service location. Uses SSL for privacy.	Client-Server	Yes
24601[13,14]	JBoss Transaction Services Recovery Manager port	TCP	Not used remotely.	Server	Yes

[14] The default port number. You must use the same port number for all products or hosts managed by the Management server. This port is configurable in the Management server; however, some products and firmware versions do not allow you to configure a port.
[13] Port does not need to be open in the firewall for Professional edition.

TABLE 15 Port usage and firewall requirements (continued)

Port number	Ports	Transport	Description	Communication path	Open in firewall
24602[13],[14]	JBoss Transaction Status Manager port	TCP	Not used remotely.	Server	Yes
24603[13],[14]	HornetQ Netty port	TCP	Use for JMS (Java Message Service), async messages from server to client. Uses SSL for privacy.	Client-Server	Yes
24604[13],[14]	JMX remoting connector port	TCP	Management console port for native connector (JMX).	Client-Server	Yes
24605[13],[14]	JBoss HTTPS management port	TCP	Management console port for HTTPS-based management.	Client-Server	Yes
24606[13],[14]	Fault management CIM indication listener port	TCP	Used for HBA management.	Managed Host-Server	Yes
24607[13],[14]	HCM proxy CIM indication listener port	TCP	Used for HBA management.	Managed Host-Server	Yes
24608[14]	Reserved for future use	TCP	Not used.	Client-Server	No
24609[14]	Reserved for future use	TCP	Not used.	Client-Server	No
24610[14]	Reserved for future use	TCP	Not used.	Client-Server	No
34568	HCM agent discovery port	TCP	Used for HBA management via JSON.	Server-Managed Host	Yes
55556[13]	Launch in Context (LIC) client hand-shaking port	TCP	Client port used to check if a Management application client that opened using LIC is running on the same host. NOTE If this port is in use, the application uses the next available port.	Client	No

Edition feature support

The following table details whether the features are supported in the Professional, Professional Plus, or Enterprise versions, or only through the Element Manager of the device.

[13] Port does not need to be open in the firewall for Professional edition.
[14] The default port number. You must use the same port number for all products or hosts managed by the Management server. This port is configurable in the Management server; however, some products and firmware versions do not allow you to configure a port.

TABLE 16 SAN features supported

Feature	Professional	Professional Plus	Enterprise
AAA (Authentication, authorization, and accounting) Authentication and authorization configuration	No	Yes	Yes
Access Gateway (AG) management			
AG display	Yes	Yes	Yes
Support for firmware download, supportSave, performance statistics, and configuration file management	Yes	Yes	Yes
Active session management	Yes	Yes	Yes
Bottleneck detection			
Badge on topology and product tree	Yes	Yes	Yes
Configuration	No	Yes	Yes
Show affected host	No	Yes	Yes
Statistics	No	Yes	Yes
Call Home support			
Support for all call home centers	No	Yes	Yes
Support for appending the last 30 events in a call home event for e-mail-based call home centers	No	Yes	Yes
SupportSave for Fabric OS switches	No	Yes	Yes
Certificate management	No	Yes	Yes
COMPASS	No	Yes	Yes
Configuration management			
Configuration repository management	No	Yes	Yes
Firmware download	Yes	Yes	Yes
Manual backup **NOTE** Professional only supports one switch at a time.	Yes	Yes	Yes
Periodic configuration backup and persistence	No	Yes	Yes
Replicate switch configuration	No	Yes	Yes
Save configuration **NOTE** Professional only supports one switch at a time.	Yes	Yes	Yes
Dashboard	Yes	Yes	Yes

TABLE 16 SAN features supported (continued)

Feature	Professional	Professional Plus	Enterprise
DCB configuration management	Yes	Yes	Yes
SAN768B backbone chassis discovery and management	No	No	Yes
Diagnostic port test	No	Yes	Yes
Digital diagnostic	Yes	Yes	Yes
Encryption			
Access Gateway - Cisco interop support	Yes	Yes	Yes
Device decommissioning	Yes	Yes	Yes
Encryption configuration and monitoring	Yes	Yes	Yes
Layer 2 FC support	Yes	Yes	Yes
End device connectivity Collection Views	Yes	Yes	Yes
Fabric binding	No	Yes	Yes
Fabric Watch			
Admin	Element Manager	Element Manager	Element Manager
Hardware	Element Manager	Element Manager	Element Manager
Name Server	Element Manager	Element Manager	Element Manager
Ports	Element Manager	Element Manager	Element Manager
Router Admin	Element Manager	Element Manager	Element Manager
Fault management			
Common SNMP/trap registration	No	Yes	Yes
Event forwarding	No	Yes	Yes
Event custom report	No	Yes	Yes
Event processing (event policies and pseudo events)	Yes	Yes	Yes
Show switch events	Yes	Yes	Yes
Show fabric events	Yes	Yes	Yes
SNMP trap registration and forwarding	Yes	Yes	Yes
Syslog registration and forwarding	Yes	Yes	Yes
Trap configuration, credentials, and customization	Yes	Yes	Yes
FCIP management			
FCIP configuration wizard	Yes	Yes	Yes
Iperf and IP trace route	Yes	Yes	Yes
FCoE management			
FCoE configuration	Yes	Yes	Yes
Migration from DCFM	Yes	Yes	Yes
FICON/CUP			

TABLE 16 SAN features supported (continued)

Feature	Professional	Professional Plus	Enterprise
Cascaded FICON configuration wizard	No	No	Yes
Cascaded FICON fabric merge wizard	No	No	Yes
PDCM Matrix	Element Manager	Element Manager	Yes
Firmware management and supportSave			
Capture SupportSave	Yes	Yes	Yes
Firmware download	Yes	Yes	Yes
Flow Vision	No	Yes	Yes
Flow Vision - NVMe	No	Yes	Yes
Frame monitor	No	Yes	Yes
HBA management			
Driver/DIOS management	No	Yes	Yes
Fabric-assigned WWN	No	Yes	Yes
HBA management	Yes	Yes	Yes
VM management	Yes	Yes	Yes
HBA server and storage port mapping	No	Yes	Yes
High Integrity Fabric	No	Yes	Yes
IPv6 - Server - Switch support	Yes	Yes	Yes
iSCSI discovery	Yes	Yes	Yes
Layer 2 trace route	No	Yes	Yes
License	No	Yes	Yes
MAPS management	No	Yes	Yes
Meta-SAN Domain ID configuration Routing configuration	No	Yes	Yes
Name Server	Yes	Yes	Yes
Open Trunking Support			
Display trunks on the topology	Yes	Yes	Yes
Display trunks properties	Yes	Yes	Yes
Display marching ants	Yes	Yes	Yes
Display connection properties	Yes	Yes	Yes
Performance management - SNMP monitoring			
Data aging	No	Yes	Yes
End-to-end monitors	No	Yes	Yes
Historical Performance collection, display, and reports	No	Yes	Yes
Marching ants	No	Yes	Yes
Real Time Performance collection, display, and reports	Yes	Yes	Yes

TABLE 16 SAN features supported (continued)

Feature	Professional	Professional Plus	Enterprise
Thresholds	No	Yes	Yes
Top talkers - Supported on SAN switches and Access Gateway	No	Yes	Yes
Policy Monitor	Yes	Yes	Yes
Port administration	Element Manager	Element Manager	Element Manager
Port fencing	No	Yes	Yes
Port group configuration	No	No	Yes
Reports	Yes	Yes	Yes
FCR reports	Yes	Yes	Yes
Generate reports	Yes	Yes	Yes
Performance reports	Yes	Yes	Yes
View reports	Yes	Yes	Yes
SCOM plug-in support	No	Yes	Yes
Security management			
L2 ACL configuration **NOTE** Supported only on DCB devices.	Yes	Yes	Yes
Replicate switch policy configuration	No	Yes	Yes
SNMP configuration	Yes	Yes	Yes
SMI Agent Access Points Sub Profile CEE (Converged Enhanced Ethernet) CP Blade Sub Profile Enhanced Zoning and Enhanced Zoning Control Sub Profile Fabric and Host Discovery Fabric Profile Fabric Switch Partitioning Sub Profile Fabrics Virtual Fabrics Sub Profile Fabric Views Sub Profile FC Initiator Ports Sub Profile FC HBA (Fibre Channel Host Bus Adapter) Profile Fan, Power Supply, and Sensor Profiles Inter Fabric Routing (FCR) Profile FDMI (Fabric Device Management Interface) Sub Profile Indication Sub Profile Launch In Context Profile	No	Yes	Yes

TABLE 16 SAN features supported (continued)

Feature	Professional	Professional Plus	Enterprise
Location Sub Profile N Port Virtualizer (AG NPIV) Profile Object Manager Adapter Sub Profile Physical Package Sub Profile Profile Registration Sub Profile Role Based Authorization (CEE ACL) Profile SAN Zoning Server Profile Software Sub Profile Switch Profile Topology View Sub Profile Trunking Zone Control Sub Profile			
Switch configuration management Basic configurations through the Element Manager	Yes	Yes	Yes
Switch port enable/disable through right-click menu	Yes	Yes	Yes
Technical SupportSave	Yes	Yes	Yes
Telnet NOTE Telnet through the server is supported only on Windows systems.	Yes	Yes	Yes
Tools launcher (Setup Tools)	No	Yes	Yes
Troubleshooting and Diagnostics			
Device connectivity troubleshooting wizard	Yes	Yes	Yes
Fabric device sharing	No	Yes	Yes
Trace route and ping	Yes	Yes	Yes
User management	No	Yes	Yes
View management	No	Yes	Yes
Virtual fabric support			
Configuration	No	Yes	Yes
Discovery	Yes	Yes	Yes
VLAN management	Yes	Yes	Yes
VM plugin support	No	Yes	Yes
Web Element Manager	Yes	Yes	Yes
Zoning			

TABLE 16 SAN features supported (continued)

Feature	Professional	Professional Plus	Enterprise
Delete zone database	No	Yes	Yes
Device to zone/ zoneset participation analysis	Yes	Yes	Yes
Impact analysis	Yes	Yes	Yes
Import or export a zone database	No	Yes	Yes
LSAN zones	No	Yes	Yes
Live fabric library scope	Yes	Yes	Yes
Member selection	Yes	Yes	Yes
QoS support	Yes	Yes	Yes
Remove offline devices	No	Yes	Yes
Rolling back to an activated zone database	No	Yes	Yes
TI zones	Yes	Yes	Yes
Zone alias support	Yes	Yes	Yes
Zone editing	Yes	Yes	Yes

The following table details whether the IP features are fully or partially supported in the Professional or Licensed versions.

TABLE 17 IP features supported

Feature	Professional	Base Licensed version	Base with Licensed Ethernet Fabrics	Base with Unlicensed Ethernet Fabrics
802.1ag support (MPLS and VLAN management)	No	Yes	Yes	Yes
AAA (Authentication, Authorization, and Accounting) Authentication and authorization configuration	No	Yes	Yes	Yes
Address Finder	No	Yes	Yes	Yes
ADP management	No	Yes	Yes	Yes
AMPP (port profile)	No	Yes	Yes	No
Call Home support				
Support for all call home centers	No	Yes	Yes	Yes
Support for appending the last 30 events in a call home event for e-mail-based call home centers	No	Yes	Yes	Yes
Change management	Partial support	Yes	Yes	Yes
CLI configuration management	No	Yes	Yes	Yes
CLI Element Manager	Yes	Yes	Yes	Yes
Configuration management				
Configuration snapshot	No	Yes	Yes	Yes

TABLE 17 IP features supported (continued)

Feature	Professional	Base Licensed version	Base with Licensed Ethernet Fabrics	Base with Unlicensed Ethernet Fabrics
Configuration repository management	Yes	Yes	Yes	Yes
Manual backup **NOTE** Professional only supports one product at a time.	Yes	Yes	Yes	Yes
Save configuration **NOTE** Professional only supports one switch at a time.	Yes	Yes	Yes	Yes
Save configuration for VCS-enabled switches	No	Yes	Yes	Yes
Periodic configuration backup and persistence	No	Yes	Yes	Yes
Replicate switch configuration	No	Yes	Yes	Yes
Product configuration • Setting baselines • Search	No	Yes	Yes	Yes
Change tracking	No	Yes	Yes	Yes
Configuration wizard				
Product configuration - create, edit, and deploy	Yes	Yes	Yes	Yes
Interface payload - sFlow configuration **NOTE** Professional only supports one product at a time.	Yes	Yes	Yes	Yes
Product Payloads: • CLI configuration • CLI product monitoring	No	Yes	Yes	Yes
Dashboard	Yes	Yes	Yes	Yes
DCB configuration management	Yes	Yes	Yes	Yes
Deployment management	Yes	Yes	Yes	Yes
Discovery				
IP discovery	Yes	Yes	Yes	Yes
VCS discovery	Yes	Yes	Yes	Yes

TABLE 17 IP features supported (continued)

Feature	Professional	Base Licensed version	Base with Licensed Ethernet Fabrics	Base with Unlicensed Ethernet Fabrics
NOTE Professional supports one cluster member.				
Fabric Watch **NOTE** Only supported on DCB switches.				
Hardware	Element Manager	Element Manager	Element Manager	Element Manager
Ports	Element Manager	Element Manager	Element Manager	Element Manager
Admin	Element Manager	Element Manager	Element Manager	Element Manager
Router Admin	Element Manager	Element Manager	Element Manager	Element Manager
Name Server	Element Manager	Element Manager	Element Manager	Element Manager
Fault Management				
Show switch events	Yes	Yes	Yes	Yes
Syslog registration and forwarding	Yes	Yes	Yes	Yes
SNMP trap registration and forwarding	Yes	Yes	Yes	Yes
Trap configuration, credentials, and customization	Yes	Yes	Yes	Yes
Event forwarding	No	Yes	Yes	Yes
Event custom report	No	Yes	Yes	Yes
Event processing (event policies and pseudo events)	No	Yes	Yes	Yes
Common SNMP/Trap registration	Yes	Yes	Yes	Yes
FCoE configuration management	Yes	Yes	Yes	Yes
Firmware Management and SupportSave				
Firmware download	Yes	Yes	Yes	Yes
Capture SupportSave	Yes	Yes	Yes	Yes
GSLB management	No	Yes	Yes	Yes
HBA management				
HBA management	Yes	Yes	Yes	Yes
VM management	No	Yes	Yes	Yes
Driver/DIOS management	No	No	No	No
Fabric assigned WWN	No	No	No	No
IPv6 Server - Product support	Yes	Yes	Yes	Yes

TABLE 17 IP features supported (continued)

Feature	Professional	Base Licensed version	Base with Licensed Ethernet Fabrics	Base with Unlicensed Ethernet Fabrics
NOTE Only supported in the application when IPv6 is supported on the product.				
Layer 2 trace route	No	Yes	Yes	No
License	No	Yes	Yes	Yes
MLX/XMR management	No	Yes	Yes	Yes
MPLS management	No	Yes	Yes	Yes
LSP	No	Yes	Yes	Yes
VCID pool	No	Yes	Yes	Yes
VLL manager	No	Yes	Yes	Yes
VLL monitor	No	Yes	Yes	Yes
VPLS manager	No	Yes	Yes	Yes
VPLS monitor	No	Yes	Yes	Yes
Performance management - SNMP monitoring				
Real Time Performance collection, display, and reports	Yes	Yes	Yes	Yes
Historical Performance collection, display, and reports	No	Yes	Yes	Yes
Thresholds	No	Yes	Yes	Yes
Data aging	No	Yes	Yes	Yes
Performance management - Traffic Analysis (sFlow)				
sFlow configuration payload (configuration wizard)	No	Yes	Yes	Yes
Monitoring reports	No	Yes	Yes	No
Accounting reports	No	Yes	Yes	Yes
Custom reports	No	Yes	Yes	Yes
Policy Monitor	Yes	Yes	Yes	Yes
Power Center	Yes	Yes	Yes	Yes
Reports				
IP product inventory report	Yes	Yes	Yes	Yes
SSL Certificate management	No	Yes	Yes	Yes
Third Party Device support	No	Yes	Yes	Yes
Security management				
MAC filter configuration	Yes	Yes	Yes	Yes
L2 ACL configuration	Yes	Yes	Yes	Yes

TABLE 17 IP features supported (continued)

Feature	Professional	Base Licensed version	Base with Licensed Ethernet Fabrics	Base with Unlicensed Ethernet Fabrics
L3 ACL configuration	Yes	Yes	Yes	Yes
Services	Yes	Yes	Yes	Yes
Networks	Yes	Yes	Yes	Yes
Switch configuration management Basic configurations through the Element Manager	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
Tools launcher (Setup Tools)	No	Yes	Yes	Yes
Topology management	Yes	Yes	Yes	Yes
User Management	No	Yes	Yes	Yes
VCS Trace Route				
Trace route	Yes	Yes	Yes	Yes
Historical Graphs/Tables	No	Yes	Yes	Yes
VIP Server management	No	Yes	Yes	Yes
VLAN management	Yes	Yes	Yes	Yes
VM Plugin Support	No	Yes	Yes	Yes
Web Element Manager	Yes	Yes	Yes	Yes
Web Tools/Fabric Watch	Yes	Yes	Yes	Yes
Zoning				
Member selection	Yes	Yes	Yes	Yes
Zone editing	Yes	Yes	Yes	Yes
Live fabric library scope	Yes	Yes	Yes	Yes
Zone alias support	Yes	Yes	Yes	Yes
Delete Zone database	No	Yes	Yes	Yes
Impact analysis	Yes	Yes	Yes	Yes
Remove offline devices	No	Yes	Yes	Yes
Device to Zone / zoneset participation analysis	Yes	Yes	Yes	Yes
LSAN Zones	No	Yes	Yes	Yes
Rolling back to an activated zone database	No	Yes	Yes	Yes
Import or export a zone database	No	Yes	Yes	Yes

Printed in USA

GC27-6622-04