

53-1002801-01
17 December 2012



Brocade Network Advisor

SAN Installation and Migration Guide

Supporting Network Advisor 12.0.0

BROCADE

Copyright © 2012 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, MLX, NetIron, SAN Health, ServerIron, TurboIron, VCS, and VDX are registered trademarks, and AnyIO, Brocade One, CloudPlex, Effortless Networking, ICX, NET Health, OpenScript, and The Effortless Network are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

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

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

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

Document History

Title	Publication number	Summary of changes	Date
<i>Network Advisor SAN Installation and Migration Guide</i>	53-1002801-01	New document	December 2012

Contents

About This Document

- In this chapter v
- How this document is organized v
- Supported hardware and softwarevi
 - Fabric OS hardware and software supportvi
- What’s new in this document..... ix
- Document conventions..... x
 - Text formatting x
 - Notes..... x
 - Key terms x
- Notice to the reader xi
- Additional information..... xi
 - Brocade resources.....xi
 - Other industry resources.....xi
- Getting technical help..... xii
- Document feedback xiii

Chapter 1

Installation

- System requirements1
 - Server and Client operating system requirements2
 - Host requirements.....3
 - Memory requirements.....3
 - Operating system cache requirements4
 - Disk space requirements4
 - Browser requirements.....5
 - Client and server system requirements6
- Pre-installation requirements.....6
 - Additional pre-installation requirements for UNIX systems.....7
- Installing the application8
 - Mapping the loopback address to the localhost.....9
- Headless installation10
 - Additional pre-installation requirements for UNIX systems (headless installation)10
 - Performing a headless installation on Windows and UNIX systems11
 - Troubleshooting the Linux headless installation11

Chapter 2	Network Advisor Configuration	
	Configuring Network Advisor	13
	Accessing the Network Advisor interfaces	19
	Logging into a server	19
	Launching a remote client.	20
	Launching the SMC on Linux	21
	Launching the SMIA Configuration Tool	21
	Launching the SMIA Configuration Tool remote client	21
	Syslog troubleshooting	22
	Finding the process	22
	Stopping the process.	22
	Installing the ODBC driver.	23
	Installing the ODBC driver on Windows systems	23
	Installing the ODBC driver on Linux systems	24
	Smart Card driver installation	27
	Installing the Smart Card driver on the local client	27
	Installing the Smart Card driver on the remote client	29
	Detecting and correcting a default Linux Smart Card driver.	29
	Configuring an explicit server IP address	31
	Configuring remote client access to the database.	32
Chapter 3	Data Migration	
	Upgrading the license.	33
	Supported migration paths.	34
	DCFM migration paths.	36
	EFCM and Fabric Manager migration paths	36
	Pre-migration requirements	36
	Pre-migration requirements when migrating from one server to another	37
	Additional pre-migration requirements on UNIX systems	38
	Additional trial requirements.	39
	Migrating data	39
Chapter 4	Uninstallation	
	Uninstalling from Windows systems	47
	Uninstalling from Windows systems (headless uninstall)	48
	Uninstalling from UNIX systems	48
	Uninstalling from UNIX systems (headless uninstall)	49

Appendix A

References

Network Advisor packages51
Edition feature support.....52
Management server and client ports58
Scalability limits61

About This Document

In this chapter

- [How this document is organized](#) v
- [Supported hardware and software](#)..... vi
- [What's new in this document](#)..... ix
- [Document conventions](#) x
- [Notice to the reader](#) xi
- [Additional information](#)..... xi
- [Getting technical help](#)..... xii
- [Document feedback](#) xiii

How this document is organized

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

The document contains the following components:

- [Chapter 1, "Installation,"](#) provides system and pre-installation requirements as well as step-by-step installation instructions.
- [Chapter 2, "Network Advisor Configuration,"](#) provides step-by-step instructions to configure a fresh Network Advisor installation.
- [Chapter 3, "Data Migration,"](#) provides pre-migration requirements as well as step-by-step instructions for migrating data from a previous release of Network Advisor.
- [Chapter 4, "Uninstallation,"](#) provides step-by-step instructions for performing a partial or full uninstall of Network Advisor.
- [Appendix A, "References,"](#) provides the following information for quick lookup.
 - [Network Advisor packages](#)
 - [Edition feature support](#)
 - [Management server and client ports](#)
 - [Scalability limits](#)

Supported hardware and software

In those instances in which procedures or parts of procedures documented here 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 Network Advisor 12.0.X, documenting all possible configurations and scenarios is beyond the scope of this document.

Fabric OS hardware and software support

The following firmware platforms are supported by this release of Network Advisor 12.0.X:

- Fabric OS 5.0 or later in a pure Fabric OS fabric
- Fabric OS 6.0 or later in a mixed fabric

NOTE

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

The hardware platforms in the following table are supported by this release of Network Advisor 12.0.X.

TABLE 1 Fabric OS-supported hardware

Device name	Terminology used in documentation	Firmware level required
Brocade 200E switch	16-port, 4 Gbps FC Switch	
Brocade 300 switch	24-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
Brocade 4012 switch	Embedded 12-port, 4 Gbps FC Switch	
Brocade 4016 switch	Embedded 16-port, 4 Gbps FC Switch	
Brocade 4018 switch	Embedded 18-port, 4 Gbps FC Switch	
Brocade 4020 switch	Embedded 20-port, 4 Gbps FC Switch	
Brocade 4024 switch	Embedded 24-port, 4 Gbps FC Switch	Fabric OS v5.3.1 or later
Brocade 4100 switch	32-port, 4 Gbps FC Switch	
Brocade 4900 switch	64-port, 4 Gbps FC Switch	Fabric OS v5.2.0 or later
Brocade 5000 switch	32-port, 4 Gbps FC Interop Switch	Fabric OS v5.2.1 or later
Brocade 5100 switch	40-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
Brocade 5300 switch	80-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
Brocade 5410 embedded switch	Embedded 12-port, 8 Gbps Switch	Fabric OS v6.1.0 or later
Brocade M5424 embedded switch	Embedded 24-port, 8 Gbps Switch	
Brocade 5450 embedded switch	Embedded 16-port, 8 Gbps Switch	
Brocade 5460 embedded switch	Embedded 24-port, 8 Gbps Switch	
Brocade 5470 embedded switch	Embedded 24-port, 8 Gbps Switch	
Brocade 5480 embedded switch	Embedded 24-port, 8 Gbps Switch	Fabric OS v6.1.0 or later
Brocade 6505 switch	24-port, 16 Gbps Edge switch	Fabric OS v7.0.1 or later

TABLE 1 Fabric OS-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
Brocade 6510 switch	48-port, 16 Gbps switch	Fabric OS v7.0.0 or later
Brocade 7500 Extension switch	4 Gbps Router, Extension Switch	Fabric OS v5.1.0 or later
Brocade 7500E Extension switch	4 Gbps Extension Switch	Fabric OS v5.1.0 or later
FR4-18i Blade	4 Gbps Router, Extension blades	
Brocade AP7600 switch	4 Gbps 32-port Switch	Fabric OS v6.1.0 or later
Brocade 7800 switch	8 Gbps Extension Switch	Fabric OS v6.3.0 or later
Brocade 8000 switch	8 Gbps 8-FC port, 10 GbE 24-DCB port Switch	Fabric OS v6.1.2_CEE
Brocade 8470 FCoE embedded switch	FCoE Embedded Switch	Fabric OS v6.3.1_CEE
Brocade VA-40FC switch	8 Gbps 40-port Switch	
Brocade 415 Host Bus Adapter	4 Gbps 1-port HBA	
Brocade 425 Host Bus Adapter	4 Gbps 2-port HBA	
Brocade 815 Host Bus Adapter	8 Gbps 1-port HBA	
Brocade 825 Host Bus Adapter	8 Gbps 2-port HBA	
Brocade 1860 Fabric Adapter	16 Gbps FC HBA mode 10 Gbps CNA mode 10 Gbps NIC mode	Adapter Software 3.0.0.0 or later
Brocade 1867 HBA	16 Gbps Mezzanine HBA	Adapter Software 3.0.3.0 or later
Brocade 48000 director	Director Chassis	
Brocade 48000 director with FC4-16, FC4-32, and FC4-48 Blades	Director Chassis with 4 Gbps 16-FC port, 4 Gbps 32-FC port, and 4 Gbps 48-FC port	Fabric OS v5.2.0 or later (FC4-48)
Brocade 48000 director with FR4-18i Blades	Director Chassis with 4 Gbps router, extension blades	Fabric OS v5.1.0 or later (FR4-18i)
Brocade 48000 director with FC4-16IP Blades	Director Chassis with 4 Gbps 8-FC port and 8 GbE iSCSI blades	Fabric OS v5.2.0 or later (FC4-16IP)
Brocade 48000 director with FC10-6 Blades	Director Chassis with 10 Gbps 6-port ISL blades	Fabric OS v5.3.0 or later (FC10-6)
Brocade DCX ^{1, 2}	8-slot Backbone Chassis	Fabric OS v6.0.0 or later
Brocade DCX ^{<superscript>1, <superscript>2} with FC8-16, FC8-32, and FC8-48 Blades	8-slot Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades	Fabric OS v6.0.0 or later
Brocade DCX ^{<superscript>1, <superscript>2} with FC8-64 Blades	8-slot Backbone Chassis with 8 Gbps 64-FC port blades	Fabric OS v6.4.0
Brocade DCX ^{<superscript>1, <superscript>2} with FR4-18i Blades	8-slot Backbone Chassis with 4 Gbps Router, Extension blade	Fabric OS v6.0.0 or later
Brocade DCX ^{<superscript>1, <superscript>2} with FC10-6 Blades	8-slot Backbone Chassis with FC 10 - 6 ISL Blade	Fabric OS v6.2.0
Brocade DCX ^{<superscript>1, <superscript>2} with FS8-18 Blades	8-slot Backbone Chassis with Encryption Blade	Fabric OS v6.1.1_enc or later
Brocade DCX ^{<superscript>1, <superscript>2} with FX8-24 Blades	8-slot Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade	Fabric OS v6.3.1_CEE

TABLE 1 Fabric OS-supported hardware (Continued)

Device name	Terminology used in documentation	Firmware level required
Brocade DCX ¹ , ² with FCoE10-24 Blades	8-slot Backbone Chassis with 10 Gbps 24-port FCoE blade	Fabric OS v6.3.1_CEE
Brocade DCX-4S	4-slot Backbone Chassis	Fabric OS v6.0.0 or later
Brocade DCX-4S with FC8-16, FC8-32, and FC8-48 Blades	4-slot Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades	Fabric OS v6.2.0
Brocade DCX-4S with FC8-64 Blades	4-slot Backbone Chassis with 8 Gbps 64-FC port blades	Fabric OS v6.4.0
Brocade DCX-4S with FR4-18i Blades	4-slot Backbone Chassis with 4 Gbps Router, Extension blade	Fabric OS v6.2.0
Brocade DCX-4S with FC10-6 Blades	4-slot Backbone Chassis with FC 10 - 6 ISL Blade	Fabric OS v6.2.0
Brocade DCX-4S with FS8-18 Blades	4-slot Backbone Chassis with Encryption Blade	Fabric OS v6.1.1_enc or later
Brocade DCX-4S with FX8-24 Blades	4-slot Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade	Fabric OS v6.3.1_CEE
Brocade DCX-4S with FCoE10-24 Blades	4-slot Backbone Chassis with 10 Gbps 24-port FCoE blade	Fabric OS v6.3.0 or later
Brocade DCX 8510-4	16 Gbps 4-slot Backbone Chassis	Fabric OS v7.0.0 or later
Brocade DCX 8510-8 ¹ , ²	16 Gbps 8-slot Backbone Chassis	Fabric OS v7.0.0 or later
Brocade Encryption Switch	8 Gbps Encryption Switch	Fabric OS v6.1.1_enc or later
FS8-18 Encryption Blade	Encryption Blade	
FA4-18 Application Platform Blade	Application Platform Blade	
FC8-16 Blade	FC 8 GB 16-port Blade	
FC8-32 Blade	FC 8 GB 32-port Blade	
FC8-48 Blade	FC 8 GB 48-port Blade	
FC8-64 Blade	FC 8 GB 64-port Blade	
FC10-6 Blade	FC 10 - 6 ISL Blade	
FC8-32E blade ³	8 Gbps 32-port blade	Fabric OS v7.0.1 or later
FC8-48E blade ³	8 Gbps 48-port blade	Fabric OS v7.0.1 or later
FC16-32 Blade	16 Gbps 32-port blade	Fabric OS v7.0.0 or later
FC16-48 Blade	16 Gbps 48-port blade	Fabric OS v7.0.0 or later
FCoE10-24 Blade	10 Gbps FCoE Port Router Blade	
FX8-24 Blade ¹ , ²	8 Gbps Extension Blade	

1. Professional can discover, but not manage this device. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.
2. Professional Plus Trial and Licensed version can discover, but not manage, this device. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.
3. Only supported on the DCX 8510-4 and DCX 8510-8 chassis.

What's new in this document

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

- Information that was added:
 - Documented OS cache requirements (refer to [“Operating system cache requirements”](#) on page 4)
 - Documented Linux 64-bit troubleshooting (refer to [“Testing the connection on Linux systems”](#) on page 25)
 - Documented unsupported migration work arounds (refer to [“Pre-migration requirements”](#) on page 36).
- Information that was changed:
 - Updated server and client operating system details (refer to [“Server and Client operating system requirements”](#) on page 2)
 - Updated the Java-Plug-ins ([“Browser requirements”](#) on page 5)
 - Updated the number of clients allowed ([“Client and server system requirements”](#) on page 6)
 - Updated configuration procedure ([“Configuring Network Advisor”](#) on page 13)
 - Updated accessing the interface procedures ([“Accessing the Network Advisor interfaces”](#) on page 19)
 - Updated Linux ODBC driver procedure ([“Installing the ODBC driver on Linux systems”](#) on page 24)
 - Updated migration paths ([“Supported migration paths”](#) on page 34)
- Information that was deleted:
 - None.

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

Document conventions

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

Text formatting

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

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
<code>code text</code>	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is all lowercase.

Notes

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

NOTE

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

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See "[Brocade resources](#)" on page xi for instructions on accessing MyBrocade.

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

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

Notice to the reader

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

These references are made for informational purposes only.

Corporation	Referenced trademarks and products
Linus Torvalds	Linux
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Sun Microsystems, Inc.	Sun, Solaris, Sun Fire, Sun Ultra, Java Plug-in
The Open Group	UNIX
VMware, Inc.	VMware

Additional information

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

Brocade resources

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

White papers, online demonstrations, and data sheets are available through the Brocade website at:

<http://www.brocade.com/products-solutions/products/index.page>

For additional Brocade documentation, visit the Brocade website:

<http://www.brocade.com>

Release notes are available on the MyBrocade website.

Other industry resources

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

<http://www.t11.org>

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

<http://www.fibrechannel.org>

Getting technical help

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

1. Management Application Serial Number

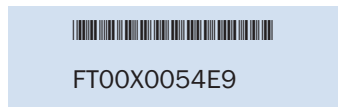
To obtain the Management application serial number, select **Help > License**. The **License** dialog box displays.

2. General Information

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

3. Switch Serial Number

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



The serial number label is located as follows:

- *Brocade 300, 4100, 4900, 5100, 5300, 7500, 7800, 8000, VA-40FC, and Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left
- *Brocade 5000*—On the switch ID pull-out tab located on the bottom of the port side of the switch
- *Brocade 7600*—On the bottom of the chassis
- *Brocade 48000*—Inside the chassis next to the power supply bays
- *Brocade DCX*—On the bottom right on the port side of the chassis
- *Brocade DCX-4S*—On the bottom right on the port side of the chassis, directly above the cable management comb

4. World Wide Name (WWN)

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

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

Document feedback

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

documentation@brocade.com

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

Installation

In this chapter

- System requirements 1
- Pre-installation requirements 6
- Installing the application 8
- Headless installation 10

System requirements

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

- Server and Client operating system requirements 2
- Host requirements 3
- Memory requirements 3
- Operating system cache requirements 4
- Disk space requirements 4
- Browser requirements 5
- Client and server system requirements 6

Server and Client operating system requirements

NOTE

The SAN with SMI Agent large installation is only supported on a 64-bit Windows® operating system.

Table 2 summarizes the required Operating Systems (OS) for servers and the packages supported by each OS version.

Table 3 summarizes the required OS for clients.

TABLE 2 Server operating system requirements

Operating system	Version	Guest OS version	Supported packages
Windows	- 2003 Server SP2 (x86 32-bit)		SAN with SMI Agent SMI Agent only
	- 2008 Server (x86 32-bit)		
	- XP Professional SP3 (x86 32-bit)		
	- 7 Professional (x86 32-bit)		
	- 2008 R2 Data Center Edition (x86 64-bit)		SAN with SMI Agent SMI Agent only
	- 2008 R2 Standard Edition (x86 64-bit)		
- 2008 R2 Enterprise Edition (x86 64-bit)			
Linux®	- RedHat Enterprise 6.1 Advanced Platform (x86 32-bit)		SAN with SMI Agent SMI Agent only
	- SuSE Enterprise Server 11 (x86 32-bit)		
	- Oracle Enterprise 6.1 (x86 32-bit)		
Guest VMs	- VMware® ESX Server i 5.0 ¹	Supports all server OS versions available for Windows and Linux.	Supports all packages available for Windows and Linux.
	- Microsoft Hyper-V (Hyper-V Server 2008 R2 SP1)		
	- KVM		

1. It is recommended that you run all Network Advisor virtual CPUs on a single physical CPU.

Host requirements

TABLE 3 Client operating system requirements

Operating system	Version	Guest OS version
Windows	<ul style="list-style-type: none"> - 2003 Server SP2 (x86 32-bit) - 2008 Server (x86 32-bit) - XP Professional SP3 (x86 32-bit) - 7 Professional (x86 32-bit) 	
Linux	<ul style="list-style-type: none"> - RedHat Enterprise 6.1 Advanced Platform (x86 32-bit/64-bit) - SuSE Enterprise Server 11 (x86 32-bit) - Oracle Enterprise 6.1 (x86 32-bit) 	
Guest VMs	<ul style="list-style-type: none"> - VMware® ESX Server i 5.0 - Microsoft Hyper-V (Hyper-V Server 2008 R2 SP1) - KVM 	Supports all client OS versions available for Windows and Linux.

[Table 4](#) summarizes the minimum host requirements for running Network Advisor SAN with SMI Agent on Windows and Linux systems.

TABLE 4 SAN with SMI Agent host requirements

	Professional	Professional Plus	Enterprise		
			Small	Medium	Large LAN
Server plus one local client	Intel Core2 duo 2 GHz or equivalent	Intel Core2 duo 2 GHz or equivalent	Intel Core2 duo 2 GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent
Remote client only	N/A	Intel Core2 duo 2 GHz or equivalent	Intel Core2 duo 2 GHz or equivalent	Intel Core2 duo 2 GHz or equivalent	Intel Core2 duo 2 GHz or equivalent

[Table 5](#) summarizes the minimum host requirements for running SMI Agent only on Windows and Linux systems.

TABLE 5 SMI Agent only host requirements

	Enterprise		
	Small	Medium	Large
Server plus one local client	Intel Core2 duo 2GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent
Remote client only	Intel Core2 duo 2GHz or equivalent	Intel Core2 duo 2GHz or equivalent	Intel Core2 duo 2GHz or equivalent

Memory requirements

Table 6 summarizes the minimum system memory requirements for running Network Advisor SAN with SMI Agent on Windows and Linux systems.

TABLE 6 SAN with SMI Agent memory requirements

Server/Client	Professional	Professional Plus	Enterprise Small	Medium	Large
Server plus 1 local client	2 GB (32-bit)	3 GB (32-bit)	3 GB (32-bit)	4 GB (32-bit)	4 GB (32-bit)
	3 GB (64-bit)	4 GB (64-bit)	4 GB (64-bit)	6 GB (64-bit)	6 GB (64-bit)
Remote client only	N/A	1 GB	1 GB	2 GB	2 GB

Table 7 summarizes the minimum system memory requirements for running SMI Agent only on Windows and Linux systems.

TABLE 7 SMI Agent only memory requirements

Server/Client	Enterprise Small	Medium	Large
Server plus 1 local client	3 GB	4 GB	4 GB
Remote client only	1 GB	2 GB	2 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 use the following memory settings for your operating system.

TABLE 8 Virtual memory requirements for Windows systems

Installed physical memory (RAM) size	Windows Server 2003 SP2 and Windows XP Pro SP3		Windows Server 2008 and Windows 7 Professional	
	Minimum paging file size	Maximum paging file size	Minimum paging file size	Maximum paging file size
2 GB	2 GB	6 GB	1 GB	4 GB
3 GB	3 GB	9 GB	1 GB	4 GB
4 GB	4 GB	12 GB	1 GB	4 GB
Greater than 4 GB	N/A	N/A	1 GB	4 GB

TABLE 9 Linux swap space requirements

Installed physical memory (RAM) size	Recommended swap size
2 GB	4 GB
3 GB	4 GB
4 GB	4 GB
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

Disk space requirements

NOTE

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

Table 10 summarizes the minimum disk space requirements for running Network Advisor SAN with SMI Agent on Windows and Linux systems.

TABLE 10 SAN with SMI Agent disk space requirements

Server/Client	Professional	Professional Plus	Enterprise Small	Medium	Large
Server plus 1 local client	10 GB	10 GB	20 GB	40 GB	60 GB
Remote client only	N/A	1 GB	1 GB	1 GB	1 GB

Table 11 summarizes the minimum disk space requirements for running SMI Agent only on Windows and Linux systems.

TABLE 11 SMI Agent only disk space requirements

Server/Client	Enterprise Small	Medium	Large
Server plus 1 local client	20 GB	40 GB	60 GB
Remote client only	1 GB	1 GB	1 GB

NOTE

If you enable periodic supportSave or configure the Network Advisor server as the Upload Failure Data Capture location for monitored switches, then additional disk space will be required. 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.

Browser requirements

The launch of Network Advisor and the launch of Element Manager (Web Tools) from the application are supported from the following browsers with a Java plug-in:

- Browsers
 - Windows Internet Explorer under Windows
 - Firefox under Windows or Linux
- Java Plug-ins
 - Oracle JRE 1.7.0 update 09 for Network Advisor
 - Oracle JRE 1.7.0 update 09 for Web Tools

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

Client and server system requirements

NOTE

Network Advisor is not supported in a Network Address Translation (NAT) environment where the server and client are on different sides of the NAT Server.

Network Advisor 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 32-bit and 64-bit servers.
- 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 to 3 GB. You can configure the server memory size from the **Options** dialog box, **Memory Allocations** pane. For instructions, refer to the *Network Advisor User Manual* or online help.
 - Increase the PostgreSQL database shared buffers memory allocation to 1024 MB by editing the *Install_Home\data\databases\postgresql.conf* file.

Pre-installation requirements

Before you install Network Advisor, make sure you meet the following requirements.

- Make sure all system requirements have been met prior to installation. For specific system requirements, refer to [“System requirements”](#) on page 1.

On Windows systems, if you are running a SAN with SMI Agent large on a 32-bit machine, you must migrate to a 64-bit machine within your current release, then you can migrate to Network Advisor 12.0.

- To avoid errors, close all instances of the application before beginning the installation or uninstallation procedures.

For 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 pre-installation 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 Network Advisor 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, GNOME, and so on).
If this is a headless unit with no console, refer to [“Additional pre-installation requirements for UNIX systems \(headless installation\)”](#) on page 10.
- 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 Network Advisor server host from the X-based desktop of the remote system.
- Make sure 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 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 8).
 3. Enable the SELinux security policy using the `setenforce 1` command.

Installing the application

Before you install the application, make sure your system meets the minimum pre-installation requirements (refer to “[Pre-installation requirements](#)” on page 6). If you are migrating data, refer to “[Data Migration](#)” on page 33.

NOTE

On Windows systems, you must be an Administrator with Read and Write privileges to install Network Advisor.

NOTE

On UNIX systems, you must be the root user to install Network Advisor.

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

1. Insert the installation DVD into the DVD-ROM drive.
 - For Windows systems, if autorun is enabled, the DVD Index page launches automatically. Click the **Install** link.
If autorun is not enabled, open this file:
`DVD_Drive\Application_Name\windows\install.exe.`
 - For UNIX systems, complete the following steps.
 - a. On the Management application server, go to the following directory:
`DVD_Drive/Application_Name/UNIX_Platform/bin`
 - b. 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** screen.
3. Read the agreement on the **License Agreement** screen, 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** screen and click **Next**.

NOTE

Do not install to the root directory `C:\` (Windows) or `/` (UNIX).

5. Review the displayed installation summary on the **Pre-Installation Summary** screen and click **Install**.

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

If the localhost is not mapped to the loopback address, an error message displays. You must map the loopback address to the localhost (refer to [“Mapping the loopback address to the localhost”](#) on page 9) before you configure the application.

If the localhost 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 [“Network Advisor Configuration”](#) on page 17.
- If you are upgrading from a previous version and need to migrate data, refer to [“Data Migration”](#) on page 33.

Mapping the loopback address to the localhost

To map the loopback address to the localhost, 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 [“Network Advisor Configuration”](#) on page 17.
- If you are upgrading from a previous version and need to migrate data, refer to [“Data Migration”](#) on page 33.

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.

Before you install Network Advisor, make sure you meet the following requirements.

Make sure all system requirements have been met prior to installation. For specific system requirements, refer to “[System requirements](#)” on page 1.

Additional pre-installation requirements for UNIX systems (headless installation)

An X Server display is required, even when performing a headless installation, to run the initial configuration. Before you install Network Advisor, 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 Network Advisor 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, GNOME, and so on).

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 need to permit the remote display of the X Server by running the **xhost +IP** command, where IP is the IP address of the Network Advisor 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 might block the display to the X Server, which listens by default on TCP port 6000 on the remote host.

- Make sure 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.

Performing a headless installation on Windows and UNIX systems

To perform a headless installation through the CLI, insert the installation DVD into the DVD-ROM drive.

- For Windows systems, open a Command Prompt and execute this command:
`install.exe -i silent -DUSER_INSTALL_DIR="C:\Program Files\Network Advisor11.X.X"`
- For UNIX systems, open a UNIX shell and execute this command: `install.bin -i silent -DUSER_INSTALL_DIR="/opt/Network_Advisor11_X_X"`

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 [“Network Advisor Configuration”](#) on page 17.
- If you are upgrading from a previous version and need to migrate data, refer to [“Data Migration”](#) on page 33.

Troubleshooting the Linux headless installation

If you have completed all of the pre-Installation 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. Execute `strace -f -F -v -s 1024 -o NetworkAdvisorinstall.txt ./install.bin`.
3. Execute `rpm -qa >> system.txt`.
4. Execute `ps -elf >> system.txt`.
5. Execute `md5sum install.bin >> system.txt`.
6. Execute `df -k >> system.txt`.
7. Execute `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 from the above (containing `install.txt` and `system.txt`) to Technical Support. This file will help Technical Support isolate the issue.

1 Headless installation

Network Advisor Configuration

In this chapter

- [Configuring Network Advisor](#) 13
- [Accessing the Network Advisor interfaces](#) 19
- [Syslog troubleshooting](#) 22
- [Installing the ODBC driver](#) 23
- [Smart Card driver installation](#) 27
- [Configuring an explicit server IP address](#) 31
- [Configuring remote client access to the database](#) 32

Configuring Network Advisor

If you have not installed the application, refer to [“Installation”](#) on page 1. If you are migrating data, refer to [“Data Migration”](#) on page 33.

To configure Network Advisor, complete the following steps.

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

NOTE

You cannot migrate data to Network Advisor 12.0.X after you complete configuration.

To migrate data from a previous management application version, refer to [“Data Migration”](#) on page 33.

3. Select one of the following options on the **Package** screen and click **Next**.
 - **SAN with SMI Agent**
 - **SMI Agent Only** (Go to [step 8.](#))

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 Network Advisor client, a **License** dialog 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 affect. For instructions, refer to the user manual or online help.

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

NOTE

The DCX and DCX 8510-8 Backbone chassis require Enterprise edition.

- **Network Advisor - Licensed version**

Continue with [step 5](#). Requires you to enter a license key during configuration to enable features and configuration.

- **Network Advisor - 75 days Trial**

Go to [step 6](#). Enables you to manage SAN networks from a single interface for 75 days.

ATTENTION

If you choose to install Trial, once the trial period ends (75 days), you must upgrade to Licensed software.

- **Network Advisor - Professional**

Go to [step 6](#). Bundled with Fabric OS OS devices to manage small SAN networks from a single interface.

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

The **License Key** field is not case-sensitive.

6. Complete the following steps on the **FTP/SCP/SFTP Server** screen.
 - a. Choose one of the following options:
 - Select **Built-in FTP/SCP/SFTP Server** to configure an internal FTP/SCP/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 the *Network Advisor User Manual* or online help.
 - Select **Built-in SCP/SFTP Server** to configure an internal SCP/SFTP server
The internal SCP/SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to the *Network Advisor User Manual* or 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 the *Network Advisor User Manual* or 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 port 21 or 2221 is free and restart the Server to start the FTP/SCP/SFTP service.

NOTE

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

7. Configure the database password on the **Database Administrator Password (dcadmin)** screen by completing the following steps.
 - a. Choose one of the following options:
 - To use the default password, select **Default password**.
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 single quote (') are allowed.
 - b. Click **Next**.

You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to the *Network Advisor User Manual* or online help.

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

NOTE

If the Management server or client has multiple Network Interface Cards and if any of these 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)
- Network OS configuration backup through FTP
- 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 and Network OS products
- FTP button in Technical Support Repository dialog box
- Technical supportSave of Fabric OS, Network 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.

-
- 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 the an IPv6 address is selected, server start up will fail.

If Domain Name System (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.

If you select a specific IP address from the **Server IP Configuration** screen and the selected IP address changes, you will not be able to connect to the server. To change the IP address after configuration, refer to [“Configuring an explicit server IP address”](#) on page 31.

- c. Click **Next**.

9. Complete the following steps on the **Server Configuration** screen (Figure 1).

NOTE

Do not use port 1527 for any of these port numbers. Port 1527 is used internally by the server.

Network Advisor requires Web Server, Database, Syslog and SNMP port numbers, as well as 15 consecutive port numbers from a Starting port #. On enabling HTTP redirection, port # 80 is used to redirect the HTTP requests to HTTPS.

Web Server Port # (HTTPS)

Redirect HTTP Requests to HTTPS

Database Port #

Starting Port #

Syslog Port #

SNMP Port #

Change this configuration by selecting Server > Options > Server Port from the application.

FIGURE 1 Server Configuration screen

- 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 the *Network Advisor User Manual* or 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 Number** field (default is 24600).

NOTE

For Professional software, the server requires 15 consecutive free ports beginning with the starting port number.

NOTE

For Trial and Licensed software, the server requires 18 consecutive free ports beginning with the starting port number.

- e. Enter a port number in the **Syslog Port Number** 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, refer to "[Syslog troubleshooting](#)" on page 22.

- f. Enter a port number in the **SNMP Port Number** 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** screen 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**.

If you are configuring Professional software, go to [step 12](#).

10. Complete the following steps on the **SMI Agent Configuration** screen.
 - a. Enable the SMI Agent by selecting the **Enable SMI Agent** check box.
 - b. Enable the SLP by selecting the **Enable SLP** check box, if necessary.
Only enabled after you select the **Enable SMI Agent** check box.
 - c. Enable the SSL by selecting the **Enable SSL** check box, if necessary.
Only enabled 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 **SSL Enabled** is selected; otherwise, the default is 5988).
 - e. Click **Next**.
11. 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 9000 switch ports, 61-120 domains)**
12. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
 13. Complete the following steps on the **Start Server** screen.
 - a. (Trial and Licensed only) Select the **Start SMI Agent** check box, if necessary.
Only enabled if you enabled SMI Agent on the **SMI Agent Configuration** screen.
 - b. (Trial and Licensed only) Select the **Start SLP** check box, if necessary.
Only enabled if you enabled SLP on the **SMI Agent Configuration** screen.
 - c. Select the **Start Client** check box, if necessary.
 - d. Click **Finish**.
After all of the 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 31).

14. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively.

NOTE

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

15. Click **Login**.
16. Click **OK** on the **Network Advisor Login Banner**.

Accessing the Network Advisor interfaces

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

Logging into a server

You must log into a server to monitor your network.

NOTE

You must have an established user account on the server to log in.

1. Double-click the desktop icon or open the application from the **Start** menu.
The **Log In** dialog box displays.
2. Log into another server by entering the IP address to the other server in the **Network Address** field.

NOTE

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

3. Remove a server from the **Network Address** list by selected the IP address and clicking **Delete**.
4. Enter your user name and password.
The defaults are **Administrator** and **password**, respectively.

NOTE

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

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**.
7. Click **OK** on the **Login Banner** dialog box.
The Network Advisor application displays.

Launching a remote client

The remote client requires Oracle JRE 1.7.0_09. For the website listing patch information, go to <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

1. Open a web browser and enter the IP address of the Network Advisor server in the **Address** bar.

If the web server port number does not use the default (443 if is SSL 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*.

The Network Advisor web start screen displays.

2. Click the Network Advisor web start link.

The **Log In** dialog box displays.

3. Log into another server by entering the IP address to the other server in the **Network Address** field.

NOTE

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

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

5. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively.

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 Network Advisor application displays.

Launching the SMC on Windows

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

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

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.

1. On the Network Advisor 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**, respectively.

4. Click **Login**.

Launching the SMIA Configuration Tool remote client

The remote client requires Oracle JRE 1.7.0_09. For the website listing patch information, go to <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

1. Open a web browser and enter the IP address of the Network Advisor server in the **Address** bar.

If the web server port number does not use the default (5989 if is SSL Enabled; otherwise, the default is 5988), you must enter the web server port number in addition to the IP address. For example, *IP_Address:Port_Number*.

The Network Advisor web start screen displays.

2. Click the SMIA Configuration Tool web start link.

The **SMIA Configuration Tool Log In** dialog box displays.

3. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively.

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**.

The **SMIA Configuration Tool** displays.

Syslog troubleshooting

If the default syslog port number is already in use, you will not receive any syslog messages from the device. Use one of the following procedures (depending on your operating system), 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 Linux systems, type `netstat -nap | grep 514` and press **Enter**.
The process running on port 514 displays.
Example output: `UDP 0 0 ::ffff:127:0:0:1:514 :::* 27397.`
 - On Windows systems, type `netstat -anb | find /i "514"` and press **Enter**.
The process running on port 514 displays.
Example output: `UDP 127:0:0:1:514 *:* 3328.`

Stopping the process

Choose one of the following options:

- On Linux systems, type `kill -9 "<PID>"` and press **Enter**.
For example, `kill -9 "27397"`.
- On Windows systems, type `taskkill /F /PID "<PID>"` and press **Enter**.
For example, `taskkill /F /PID "3328"`.

OR

1. Select **Ctrl + Shift + Esc** to open Windows Task Manager.
2. Click the **Processes** tab.
3. Click the **PID** column header to sort the processes by PID.
4. Select the process you want to stop and click **End Process**.

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 Network Advisor database.

Installing the ODBC driver on Windows 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 Network Advisor database.

To install the ODBC driver, complete the following steps.

1. Double-click `edb_psqlodbc.exe` located on the DVD (*DVD_Drive/Network Advisor/odbc/Windows*).
2. Install the file to the usual location for your system's application files (for example, `C:\Program Files\Network Advisor ODBC Driver`) on the **Select Install Folder** screen 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** screen click **Next**.
4. Click **Finish** to complete the installation.
5. Choose one of the following options:
 - (32-bit OS) Select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
 - (62-bit OS) (Windows only) Select **Start > Run**, type `%windir%\SysWOW64\odbcad32.exe` and press **Enter**.

The **ODBC Data Source Administrator** dialog box displays.

6. Click the **System DSN** tab.
7. Click **Add**.

The **Create a New Data Source** dialog box displays.

8. Select **PostgreSQL Unicode**.
9. Click **Finish**.

The **PostgreSQL Unicode ODBC Driver (psqlODBC) Setup** dialog box displays.

10. Enter a name for the data source in the **Datasource** field.
11. Enter the description of the Network advisor database in the **Description** field.
12. Enter the name of the Network Advisor database in the **Database** field.
13. Select **enable** or **disable** from the **SSL Mode** list to specify whether or not to use SSL when connecting to the database.
14. Enter the IP address or host name of the Network Advisor server in the **Server** field.
15. Enter the database server port number in the **Port Number** field.

2 Installing the ODBC driver

16. Enter the database user name in the **User Name** field.
17. Enter the password in the **Password** field.
18. 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.

19. Click **OK** on the **Connection Test** dialog box.
20. Click **Save**.
21. 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 Network Advisor database.

To install the ODBC driver, complete the following steps.

1. Execute the following command in the terminal:

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

For 32-bit Linux systems, the installer file is located in DVD/BROCADE/Network Advisor/odbc/Linux/ edb_psqlodbc.bin.

For 64-bit Linux systems, the installer file is located in DVD/BROCADE/Network Advisor/odbc/Linux_64/ edb_psqlodbc.bin.

2. On the **Setup psqIODBC** screen click **Next**.
3. Install the file to the usual location for your system's application files (for example, /opt/PostgreSQL/psqIODBC) on the **Installation Directory** screen 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** screen click **Next**.
5. On the **Completing the psqIODBC Setup Wizard** screen click **Finish** to complete the installation.

Adding the Datasource on Linux systems

Before you edit the INI files, install Network Advisor (refer to “[Installation](#)” on page 1) and make sure the PostgreSQL database is up and running.

NOTE

For RedHat 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 datasource information as follows:

```
[TestDB]
Description = PostgreSQL 8.3
Driver = /opt/PostgreSQL/psqlODBC/lib/psqlodbcw.so
Database = dcldb
Servername = 172.26.1.54
UserName = dcadmin
Password = passwOrd
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` should automatically update the driver path. If the driver path is not updated, add the following:

```
[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** screen, 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** screen, complete the following steps.
 - a. Click **Browse**.
The datasource saved in the `odbc.ini` file is populated in the **Datasource** dialog box.
 - b. Select the datasource and click **OK** on the **Datasource** dialog box.
 - c. Click **Next**.

2 Installing the ODBC driver

5. On the **Set up user authentication** screen, 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 32-bit Linux systems, if an error message (file not found while testing the connection) displays, copy the lib files from the <postgresSQL path>/lib/* directory to the /usr/lib/ directory.

For 64-bit Linux systems, if an error message (cannot open library) displays, complete the following steps:

1. Execute the following command:

```
export
LD_LIBRARY_PATH=/opt/PostgreSQL/8.4/lib/:/usr/lib64/:/opt/PostgreSQL/p
sqlODBC/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 executing 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 executing the following command:

```
find -name libodbc.so*
```

5. Create a soft link for libodbc.so.1 pointing to libodbc.so.2.0.0 by executing the following command:

```
ln -s libodbc.so.1 libodbc.so.2.0.0
```

- f. Click **Next**.

6. On the **Save and proceed** screen, 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 the 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://pcsc-lite.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 Network Advisor provides the binary code on both platforms for installation. You must uncompress or untar the file depending on the platform. The procedures for the local client and the remote client configurations follow. The `thirdparty/pcsc-lite-1.4.101-linux-x86.tar.gz` file can be found on the Network Advisor 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 `pcsc` file for your platform (Linux) from the DVD and rename the file as `pcsc-lite-1.4.101-linux-x86.tar.gz` file.
3. Log in as the 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 you specified in [step 1](#).

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

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

2 Smart Card driver installation

5. Create a soft link into the system directory. This is 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 29.

6. Start the pcscd daemon 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 27.
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.

Example

```
> 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

This section applies 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 Network Advisor. Otherwise, there could be an incompatibility issue between the driver and the native library that 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 the pcscd file on 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
```

2 Smart Card driver installation

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 example below shows a different `pcscd.org` script and how to do the configuration cleanup. 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 `SNNpcscd`, 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 on `/opt/pcsc/lib` correctly. For example, to find a copy of the library on `/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 on `/usr/lib`, use the following commands.

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

Use this copy 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** screen 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 > Network Advisor 12.0.0 > Network Advisor Configuration**.
 - On UNIX systems, execute `sh Install_Home/bin/configwizard` in terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Click **Next** on the **FTP Server** screen.
5. Complete the following steps on the **Server IP Configuration** screen.
 - a. Select an address from the **Server IP Configuration** list.
 - b. Select an address from the **Switch - Server IP Configuration Preferred Address** 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 the an IPv6 address is selected, server startup will fail.

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.

- c. Click **Next**.
6. Click **Next** on the **Server Configuration** screen.
7. Click **Next** on the **SMI Agent Configuration** screen.
8. Verify your Server Name on the **Server Configuration Summary** screen and click **Next**.
9. Click **Finish** on the **Start Server** screen.
10. Click **Yes** on the restart server confirmation message.
11. Enter your user name and password and click **Login**.

The defaults are **Administrator** and **password**, respectively.

NOTE

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

12. 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

In this chapter

- [Upgrading the license](#) 33
- [Supported migration paths](#) 34
- [Pre-migration requirements](#) 36
- [Migrating data](#) 39

Upgrading the license

NOTE

You cannot upgrade the license key from Professional edition.

The quickest and simplest method of moving from one package to another is to enter the new license information on the **Network Advisor License** dialog box. The following tables list the available upgrade paths:

TABLE 12 SAN upgrade paths

Current software release	To software release
SAN Professional	SAN Professional Plus Trial or Licensed version SAN Enterprise Trial or Licensed version
SAN Professional Plus Trial	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 **Network Advisor License** dialog box displays.

2. Browse to the license file (.xml) and click **Update**.
3. Click **OK** on the **Network Advisor License** dialog box.
4. Click **OK** on the message.

The Client closes after updating the license successfully. Restart the Server, Client and 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.

3 Supported migration paths

6. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively. 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 **Network Advisor Login Banner**.

Supported migration paths

You cannot migrate directly from Network Advisor 11.0.X to Network Advisor 12.0.0. To migrate from Network Advisor 11.0.X, you must first migrate to Network Advisor 11.1.X, then migrate to Network Advisor 12.0.0. To migrate from Network Advisor 11.0.X to Network Advisor 11.1.X, refer to the *Network Advisor Migration Guide* for Network Advisor 11.1.X.

NOTE

Network Advisor 11.1.X includes 11.1.0, 11.1.1, 11.1.2, 11.1.3, 11.1.4, and 11.1.5.

NOTE

Network Advisor 11.2.X includes 11.2.0 and 11.2.1.

NOTE

Network Advisor cross flavor migration is supported pre-12.0.0 releases.

[Table 13](#) shows the migration paths from the DCFM, INM, and Network Advisor releases.

TABLE 13 Release migration path matrix

	Network Advisor			
	11.1.X	11.2.X	11.3.X	12.0.X
DCFM 10.4.X	Direct migration	DCFM 10.4.X > Network Advisor 11.1.X > Network Advisor 11.2.X	DCFM 10.4.X > Network Advisor 11.1.X > Network Advisor 11.3.X >	DCFM 10.4.X > Network Advisor 11.1.X > Network Advisor 12.0.X
INM 3.3	INM 3.3.X > Network Advisor 11.0.X > Network Advisor 11.1.X	INM 3.3.X > Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 11.2.X	INM 3.3.X > Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 11.3.X	INM 3.3.X > Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 12.0.X
Network Advisor 11.0.X,	Direct migration	Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 11.2.X	Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 11.3.X	Network Advisor 11.0.X > Network Advisor 11.1.X > Network Advisor 12.0.X
Network Advisor 11.1.X	Direct migration	Direct migration	Direct migration	Direct migration
Network Advisor 11.2.X	Not supported	Direct migration	Direct migration	Direct migration

Table 14 shows the migration paths from the Network Advisor 11.1.X, 11.2.X, 11.3.X, and 12.0.0 Professional, Trial, and Licensed versions. For the step-by-step migration procedure, refer to “Migrating data” on page 39.

TABLE 14 Network Advisor version migration paths

Current version	Professional version	Trial version		Licensed Version	
		Professional Plus	Enterprise	Professional Plus	Enterprise
Network Advisor 11.1.X/11.2.X/11.3.X Professional	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹
Network Advisor 11.1.X/11.2.X/11.3.X Professional Plus trial	No	Yes ¹	Yes ¹	Yes ¹	Yes ¹
Network Advisor 11.1.X/11.2.X/11.3.X Professional Plus Licensed	No	No	No	Yes ¹	Yes ¹
Network Advisor 11.1.X/11.2.X/11.3.X Enterprise trial	No	No	Yes ¹	No	Yes ¹
Network Advisor 11.1.X/11.2.X/11.3.X Enterprise Licensed	No	No	No	No	Yes ¹
Network Advisor 12.0.0 Professional	Yes ²	Yes ²	Yes ²	Yes ²	Yes ²
Network Advisor 12.0.0 Professional Plus trial	No	Yes ²	Yes ²	Yes ²	Yes ²
Network Advisor 12.0.0 Professional Plus Licensed	No	No	No	Yes ²	Yes ²
Network Advisor 12.0.0 Enterprise trial	No	No	Yes	No	Yes ²
Network Advisor 12.0.0 Enterprise Licensed	No	No	No	No	Yes ²

1. Migration from pre-12.0.0 releases does not support partial data migration and network path migration.
2. Local path migration is only supported when you partially uninstall the current version. Network path migration (whether the current version is fully installed or partially uninstalled) is always supported.

Table 15 shows the migration paths from SMI Agent only. For the step-by-step migration procedures, refer to “Migrating data” on page 39.

TABLE 15 SMI Agent only migration paths

Current version	Professional version	Trial version		Licensed Version		SMI Agent only
		Professional Plus	Enterprise	Professional Plus	Enterprise	
Network Advisor 11.1.X/11.2.X SMI Agent only	No	No	No	No	No	Yes
Network Advisor 11.X.0 SMI Agent only	No	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 12.0.0. You must first migrate to DCFM 10.4.X, then migrate to Network Advisor 11.1.X, then migrate to Network Advisor 12.0.0.

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 *Network Advisor Migration Guide* for Network Advisor 11.1.X.

EFCM and Fabric Manager migration paths

You cannot migrate directly from EFCM or Fabric Manager to Network Advisor 12.0.0. To migrate from EFCM or Fabric Manager, you must first migrate to DCFM 10.3.X, then migrate to Network Advisor 11.1.X, then migrate to Network Advisor 12.0.0. For more information about migrating from EFCM or Fabric Manager to DCFM 10.3.X, contact your customer representative.

Pre-migration requirements

Before you install Network Advisor, make sure you meet the following pre-migration requirements.

- Make sure all system requirements have been met prior to installation. For specific system requirements, refer to “[System requirements](#)” on page 1.
- Check for and install the latest Java patches for your operating system. Network Advisor requires Oracle JRE 1.6.0_33. 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 you close all instances of the application before migrating.
- Make sure to install Network Advisor on the same system as your current Management application.
- If you are migrating within the same release or you are migrating from Professional to Licensed software, make sure to partially uninstall (refer to “[Uninstallation](#)” on page 47) 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 Network Advisor version on the same machine and migrate the partially uninstalled data.
 2. Install Network Advisor 12.0 (refer to “[Installation](#)” on page 1) on the same machine and migrate your data (refer to “[Migrating data](#)” on page 39).

Pre-migration requirements when migrating from one server to another

- If you are migrating from a pre-12.0.0 release on a 32-bit Windows server to Network Advisor 12.0.0 on a 64-bit Windows server, complete the following steps.

NOTE

If you are migrating from DCFM 10.4.X or Network Advisor 11.0.X on a 32-bit server, first migrate to Network Advisor 11.1.X on a 32-bit server, then migrate to Network Advisor 12.0 on a 64-bit server by completing the following steps.

1. Open the Server Management Console from the **Start** menu on the 32-bit server.
2. Click **Stop** to stop all services.
3. Using Windows Explorer, browse to the 32-bit Network Advisor directory.
4. Right-click the 32-bit Network Advisor directory and select **Sharing and Security**.
5. Select the **Share this Folder** option on the **Network Advisor Properties** dialog box and click **OK**.

The folder icon changes to the shared folder icon.

6. From the 64-bit server, verify that the 32-bit server shared drive is accessible.
7. Install your current application (pre-12.0.0 release) on the 64-bit server (refer to [“Data Migration”](#) on page 33) and migrate your data ([“Migrating data”](#) on page 39).

NOTE

During migration you will need to browse to the shared directory of the 32-bit server on the **Copy Data and Settings from previous releases** screen.

8. Install Network Advisor 12.0.0 on the 64-bit Windows server (refer to [“Data Migration”](#) on page 33) and migrate your data ([“Migrating data”](#) on page 39).
- If you are migrating from a pre-12.0.0 release on a 32-bit Linux server to Network Advisor 12.0.0 on a 64-bit Linux server, complete the following steps.
 1. Install Network Advisor 12.0.0 on your current 32-bit machine (refer to [“Data Migration”](#) on page 33) and migrate your data ([“Migrating data”](#) on page 39).
 2. Back up the server data on your current machine. For instructions, refer to *“Configuring backup”* in the *Brocade Network Advisor User Manual* or online help.
 3. Install Network Advisor 12.0.0 on your new 64-bit machine (refer to [“Data Migration”](#) on page 33).
 4. Restore the server back up from your original 32-bit machine. For instructions, refer to *“Restoring data”* in the *Brocade Network Advisor User Manual* or online help.
 5. Relaunch the Configuration Wizard (refer to [“Data Migration”](#) on page 33) . For instructions, refer to *“Launching the Configuration Wizard”* in the *Brocade Network Advisor User Manual* or online help.

3 Pre-migration requirements

- If you are migrating from a Network Advisor 12.0.0 one server to another server, complete the following steps.
 1. Install Network Advisor 12.0.0 on your current machine (refer to “Data Migration” on page 33) and migrate your data (“Migrating data” on page 39).
 2. Back up the server data on your current machine. For instructions, refer to “Configuring backup” in the *Brocade Network Advisor User Manual* or online help.
 3. Install Network Advisor 12.0.0 on your new machine (refer to “Data Migration” on page 33).
 4. Restore the server back up from your original 32-bit machine. For instructions, refer to “Restoring data” in the *Brocade Network Advisor User Manual* or online help.
 5. Relaunch the Configuration Wizard (refer to “Data Migration” on page 33) . For instructions, refer to “Launching the Configuration Wizard” in the *Brocade Network Advisor User Manual* or online help.
- Cross OS migration is not supported; however, you can restore a Windows OS backup to a Linux OS and vice versa. If you are migrating from one OS to another, complete the following steps:
 1. Install Network Advisor 12.0 (refer to “Installation” on page 1) on the current machine and migrate your data (refer to “Migrating data” on page 39).
 2. Back up the server data on your current machine. For instructions, refer to “Configuring backup” in the *Brocade Network Advisor User Manual* or online help.
 3. Install Network Advisor 12.0 (refer to “Installation” on page 1) on the new machine.
 4. Restore the server back up from your original machine. For instructions, refer to “Restoring data” in the *Brocade Network Advisor User Manual* or online help.
 5. Relaunch the Configuration Wizard. For instructions, refer to “Launching the Configuration Wizard” in the *Brocade Network Advisor User Manual* or online help.

Additional pre-migration requirements on UNIX systems

- Make sure that the current application services are running.
 1. Go to *Install_Home/bin*.
 2. Execute `./smc` or `sh smc`.
 3. Click the **Services** tab.
The tab lists the DCFM 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 Network Advisor 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, GNOME, and so on).

- 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 command **xhost +IP**, where IP is the IP address of the Network Advisor server host from the X-based desktop of the remote system.

- Make sure you test the DISPLAY definition by running the command **xterm** from the same shell from which you run `install.bin`. A new X terminal window to the destination X Server display should open.

Additional trial requirements

- Two versions of the Management application (DCFM, Network Advisor, or INM) cannot reside on the same host unless there are two guest operating systems on the same 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.

Migrating data

The quickest and simplest method of moving from one package to another is to enter the new license information on the **Network Advisor License** dialog box. To upgrade from a previous release, refer to [“Upgrading the license”](#) on page 33. If you have not installed the application, refer to [“Installation”](#) on page 1.

NOTE

Trial to Professional software migration is not supported.

NOTE

Licensed software to Trial software migration is not supported.

NOTE

Enterprise software to Professional Plus software migration is not supported.

To migrate data from a previous version, complete the following steps.

1. Click **Next** on the **Welcome** screen.
2. Choose one of the following options:
 - If data is detected on your system, the **Copy Data and Settings from previous releases** screen displays. To migrate data from the previous version installed (automatically detected), select **Yes, from the following location**. Continue with [step 3](#).

- If data is not detected, the **Copy Data and Settings from previous releases** screen displays. Complete the following steps:
 - 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** screen. Continue with [step 3](#).

NOTE

If you are migrating from a 32-bit server, you will need to browse to the shared directory of the 32-bit server on the **Copy Data and Settings from previous releases** screen.

NOTE

If you are migrating to the same install location (as the previous version), you will need to browse to the renamed directory on the **Copy Data and Settings from previous releases** screen.

3. To migrate historical performance data, select the **SAN** check box, if necessary.
4. Click **Start** on the **Data Migration** screen.

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

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

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**.

NOTE

Make sure you configure the Brocade E-mail Call Home center (refer to the *Brocade Network Advisor User Manual* or online help).

If you are migrating from Professional or Trial software, continue with [step 6](#).

If you are migrating from Licensed software, go to [step 7](#).

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

NOTE

The DCX and DCX 8510-8 Backbone chassis require Enterprise edition.

- **Network Advisor - Licensed version**

Continue with [step 7](#). Requires you to enter a license key during configuration to enable features and configuration.
- **Network Advisor - 75 days Trial**

Go to [step 8](#). Enables you to manage SAN networks from a single interface for 75 days.

ATTENTION

If you choose to install Trial, once the trial period ends (75 days), you must upgrade to Licensed software.

- **Network Advisor - Professional**

Go to [step 8](#). Bundled with Fabric OS and IronWare OS devices to manage small SAN networks from a single interface.

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

- If you are migrating from a licensed source, the source license information displays. Click **Next**. Continue with [step 8](#).
- If you are migrating from Professional or Trial software to Licensed software, browse to the license file (.xml) and click **Next**. Continue with [step 8](#).

The **License Key** field is not case-sensitive.

NOTE

Downgrading the license from the current configuration during migration is not supported.

8. Complete the following steps on the **FTP/SCP/SFTP Server** screen.

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/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 the *Network Advisor User Manual* or online help.
 - Select **Built-in SCP/SFTP Server** to configure an internal SCP/SFTP server
The internal SCP/SFTP server uses a default account and port 22. You can configure your own account from the **Options** dialog box. For instructions, refer to the *Network Advisor User Manual* or 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 the *Network Advisor User Manual* or 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 port 21 or 2221 is free and restart the Server to start the FTP/SCP/SFTP service.

NOTE

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

You can configure the external FTP server settings from the **Options** dialog box. For instructions, refer to the *Network Advisor User Manual* or online help.

9. Complete the following steps on the **Server IP Configuration** screen.

NOTE

If the Management server or client has multiple Network Interface Cards and if any of these 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)
- Network OS configuration backup through FTP
- 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 and Network OS products
- FTP button in Technical Support Repository dialog box
- Technical supportSave of Fabric OS, Network 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.

-
- 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 the an IPv6 address is selected, server start up will fail.

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.

If you select a specific IP address from the **Server IP Configuration** screen 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 31.

- c. Click **Next**.

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

Network Advisor requires Web Server, Database, Syslog and SNMP port numbers, as well as 15 consecutive port numbers from a Starting port #. On enabling HTTP redirection, port # 80 is used to redirect the HTTP requests to HTTPS.

Web Server Port # (HTTPS)

Redirect HTTP Requests to HTTPS

Database Port #

Starting Port #

Syslog Port #

SNMP Port #

Change this configuration by selecting Server > Options > Server Port from the application.

FIGURE 2 Server Configuration screen

- Enter a port number in the **Web Server Port # (HTTPS)** field (default is 443).
- 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 the *Network Advisor User Manual* or online help.

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

NOTE

Do not use a port number below 1024.

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

NOTE

For Professional software, the server requires 15 consecutive free ports beginning with the starting port number.

NOTE

For Trial and Licensed software, the server requires 18 consecutive free ports beginning with the starting port number.

- 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, refer to “[Syslog troubleshooting](#)” on page 22.

- 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** screen and edit the syslog port number. Click **Yes** to close the message and continue with [step 11](#).

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**.

If you are configuring Professional software, go to [step 13](#).

- 11. Complete the following steps on the **SMI Agent Configuration** screen.
 - a. Enable the SMI Agent by selecting the **Enable SMI Agent** check box.
 - b. Enable the SLP by selecting the **Enable SLP** check box, if necessary.
Only enabled after you select the **Enable SMI Agent** check box.
 - c. Enable the SSL by selecting the **Enable SSL** check box, if necessary.
Only enabled 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 **SSL Enabled** is selected; otherwise, the default is 5988).
 - e. Click **Next**.
- 12. 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.

NOTE

If you installed the SAN with SMI Agent package on a 32-bit Windows system, the **Large** option is disabled for SAN Network Size (Enterprise).

- **Small (managing up to 2000 switch ports, 1-20 domains)**
- **Medium (managing up to 5000 switch ports, 21-60 domains)**
- **Large (managing up to 9000 switch ports, 61-120 domains)**

- 13. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
- 14. Complete the following steps on the **Start Server** screen.
 - 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 of the 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 31).

15. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively. 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.

16. Click **Login**.
17. Click **OK** on the **Network Advisor Login Banner**.

3 Migrating data

Uninstallation

In this chapter

- [Uninstalling from Windows systems](#) 47
- [Uninstalling from Windows systems \(headless uninstall\)](#) 48
- [Uninstalling from UNIX systems](#) 48
- [Uninstalling from UNIX systems \(headless uninstall\)](#) 49

This section provides step-by-step instructions to uninstall Network Advisor and SMI Agent from both Windows and UNIX systems.

NOTE

Network Advisor is installed on 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

Follow these instructions to uninstall the Network Advisor and SMI Agent from your Windows system.

1. Select **Start > Programs > Network Advisor 12.0.0 > Uninstall Network Advisor**.
2. Select one of the following options on the **Uninstall Option** screen:
 - **Partial Uninstall** – Configuration and performance data is retained to be re-used by the new installation.
 - **Full Uninstall** – All data is removed.
3. Click **Uninstall**.
4. Click **Done** on the **Uninstall Complete** screen.

Uninstalling from Windows systems (headless uninstall)

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

1. Open a command prompt.
2. Choose one of the following options:
 - To partially uninstall Network Advisor (configuration and performance data is retained to be re-used by the new installation), execute `Install_Home\Uninstall_Network Advisor 12.0.0\Uninstall_Network Advisor 12.0.0.exe -f <absolute path of partial uninstall property file>`.
 - To fully uninstall Network Advisor (all data is removed), execute `Install_Home\Uninstall_Network Advisor 12.0.0\Uninstall_Network Advisor 12.0.0.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

Follow these instructions to uninstall the Network Advisor and SMI Agent from your UNIX system.

NOTE

The Uninstall folder is retained.

1. Go to `Install_Home/Uninstall_Network_Advisor12_0_0`.
2. Execute `./Uninstall_Network_Advisor12_0_0`.
3. Select one of the following options on the **Uninstall Option** screen:
 - **Partial Uninstall** – Configuration and performance data is retained to be re-used by the new installation.
 - **Full Uninstall** – All data is removed.
4. Click **Uninstall**.
5. Click **Done** on the **Uninstall Complete** screen.

Uninstalling from UNIX systems (headless uninstall)

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

1. Go to *Install_Home/Uninstall_Network_Advisor12_0_0*.
2. Choose one of the following options:
 - To partially uninstall Network Advisor (configuration and performance data is retained to be re-used by the new installation), execute **Uninstall_Network_Advisor 12_0_0 -f <absolute path of partial uninstall property file>**.
 - To fully uninstall Network Advisor (all data is removed), execute **\Uninstall_Network_Advisor 12_0_0 -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.

4 Uninstalling from UNIX systems (headless uninstall)

References

In this Appendix

- [Network Advisor packages](#) 51
- [Edition feature support](#) 52
- [Management server and client ports](#) 58
- [Scalability limits](#) 61

Network Advisor packages

[Table 16](#) summarizes the packages and available versions for each package.

TABLE 16 Packages and versions

Package	Versions
SAN with SMI Agent	Licensed Version – Enterprise <ul style="list-style-type: none"> • SAN – Support for 36 fabrics, 10,000 devices, and 9,000 switch ports <p>NOTE:Virtual Fabrics are counted as Fabrics when calculating the managed count limits.</p>
	Licensed Version – Professional Plus <ul style="list-style-type: none"> • SAN – Support for 36 fabrics, 4,096 devices, and 2,560 switch ports <p>NOTE:Virtual Fabrics are counted as Fabrics when calculating the managed count limits.</p>
	Professional <ul style="list-style-type: none"> • SAN – Support for 1 fabric, 1,000 devices, and 1,000 ports <p>NOTE:SMI Agent is not supported on Professional.</p>

Edition feature support

Table 17 details whether the SAN features are supported in the Professional, Professional Plus, or Enterprise versions, or only through the Element Manager of the device.

TABLE 17 SAN features supported

Feature	Professional	Professional Plus	Enterprise
AAA (Authentication, Authorization, and Auditing) Authentication and authorization configuration	No	Yes	Yes
Access Gateway (AG) management			
AG display			
Support for firmware download, supportSave, performance statistics, and configuration file management	Yes	Yes	Yes
Active sessions	Yes	Yes	Yes
Bottleneck detection			
Configuration	No	Yes	Yes
Statistics	No	Yes	Yes
Badge on topology and product tree	Yes	Yes	Yes
Show affected host	No	Yes	Yes
Call Home support			
Support for all call home centers	No	Yes	Yes
SupportSave for Fabric OS switches	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
Configuration management			
Configuration repository management	No	Yes	Yes
Firmware download	Yes	Yes	Yes
Manual backup	Yes	Yes	Yes
NOTE: Professional only supports one switch at a time.			
Save configuration	Yes	Yes	Yes
NOTE: Professional only supports one switch at a time.			
Periodic configuration backup and persistence	No	Yes	Yes
Replicate switch configuration	No	Yes	Yes
Dashboard	Yes	Yes	Yes
DCB configuration management	Yes	Yes	Yes
DCX backbone chassis discovery and management	No	No	Yes
Deployment Manager			
Diagnostic port test	No	Yes	Yes
Digital diagnostic	Yes	Yes	Yes

TABLE 17 SAN features supported (Continued)

Feature	Professional	Professional Plus	Enterprise
Encryption			
Layer 2 FC support	Yes	Yes	Yes
Encryption configuration and monitoring	Yes	Yes	Yes
Access Gateway – Cisco interop support	Yes	Yes	Yes
Device decommissioning	Yes	Yes	Yes
End device connectivity	Yes	Yes	Yes
Collection			
Views			
Fabric binding	No	Yes	Yes
Fabric Watch			
Hardware	Element Manager	Element Manager	Element Manager
Ports	Element Manager	Element Manager	Element Manager
Admin	Element Manager	Element Manager	Element Manager
Router Admin	Element Manager	Element Manager	Element Manager
Name Server	Element Manager	Element Manager	Element Manager
Fault management	Element Manager	Element Manager	Element Manager
Show switch events	Yes	Yes	Yes
Show fabric events	Yes	Yes	Yes
Syslog registration and forwarding	Yes	Yes	Yes
SNMP trap registration and forwarding	Yes	Yes	Yes
Trap configuration, credentials, and customization	Yes	Yes	Yes
Event forwarding	No	Yes	Yes
Event custom report	No	Yes	Yes
Event processing (event policies and pseudo events)	No	Yes	Yes
Common SNMP/Trap registration	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
Features that support M-EOS devices and mixed fabrics	No	Yes	Yes

A Edition feature support

TABLE 17 SAN features supported (Continued)

Feature	Professional	Professional Plus	Enterprise
FICON/CUP			
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			
Firmware download	Yes	Yes	Yes
Capture SupportSave	Yes	Yes	Yes
Frame monitor	No	Yes	Yes
HBA management			
HBA management	Yes	Yes	Yes
VM management	Yes	Yes	Yes
Driver/DIOS management	No	Yes	Yes
Fabric assigned WWN	No	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
Meta-SAN	No	Yes	Yes
Routing configuration			
Domain ID configuration			
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 connections properties	Yes	Yes	Yes

TABLE 17 SAN features supported (Continued)

Feature	Professional	Professional Plus	Enterprise
Performance management - SNMP monitoring			
Real Time Performance collection, display, and reports	Yes	Yes	Yes
Historical Performance collection, display, and reports	No	Yes	Yes
Thresholds	No	Yes	Yes
Top talkers - Supported on SAN switches and Access Gateway	No	Yes	Yes
Marching ants	No	Yes	Yes
Data aging	No	Yes	Yes
End-to-End monitors	No	Yes	Yes
Policy Monitor	Yes	Yes	Yes
Port Administration	Element Manager	Element Manager	Element Manager
Port Fencing (for M-EOS switches)	No	Yes	Yes
Port group configuration	No	No	Yes
Reports	Yes	Yes	Yes
Generate reports	Yes	Yes	Yes
View reports	Yes	Yes	Yes
Performance reports	Yes	Yes	Yes
FCR reports	Yes	Yes	Yes
SCOM plug-in support	No	Yes	Yes
Security management			
Replicate switch policy configuration	No	Yes	Yes
SNMP configuration	Yes	Yes	Yes
L2 ACL configuration	Yes	Yes	Yes

NOTE: Only supported on DCB devices.

A Edition feature support

TABLE 17 SAN features supported (Continued)

Feature	Professional	Professional Plus	Enterprise
SMI Agent	No	Yes	Yes
Server Profile			
Fabric Profile			
Indication Sub Profile			
Zone Control Sub Profile			
Enhanced Zoning and Enhanced Zoning Control Sub Profile			
FDMI (Fabric Device Management Interface) Sub Profile			
Fabrics Virtual Fabrics Sub Profile			
Topology View Sub Profile			
FC HBA (Fibre Channel Host Bus Adapter) Profile			
Fan, Power Supply, and Sensor Profiles			
Inter Fabric Routing (FCR) Profile			
Trunking			
CP Blade Sub Profile			
CEE (Converged Enhanced Ethernet)			
Launch In Context Profile			
Switch Profile			
Role Based Authorization (CEE ACL) Profile			
N port Virtualizer (AG NPIV) Profile			
Profile Registration Sub Profile			
Object Manager Adapter Sub Profile			
Fabric Views Sub Profile			
Physical Package Sub Profile			
Software Sub Profile			
Access Points Sub Profile			
Location Sub Profile			
Fabric Switch Partitioning Sub Profile			
FC Initiator Ports Sub Profile			
Fabric and Host discovery			
SAN Zoning			
Switch configuration management	Yes	Yes	Yes
Basic configurations through the Element Manager			
Switch port enable/disable through right-click menu	Yes	Yes	Yes
Technical SupportSave	Yes	Yes	Yes
Telnet	Yes	Yes	Yes
NOTE: Telnet through the server is only supported on Windows systems.			
Tools launcher (Setup Tools)	No	Yes	Yes
Troubleshooting and Diagnostics			
Device connectivity troubleshooting wizard	Yes	Yes	Yes
Trace route and Ping	Yes	Yes	Yes
Fabric device sharing	No	Yes	Yes
User management	No	Yes	Yes
View management	No	Yes	Yes

TABLE 17 SAN features supported (Continued)

Feature	Professional	Professional Plus	Enterprise
Virtual fabric support			
Discovery	Yes	Yes	Yes
Configuration	No	Yes	Yes
VLAN management			
	Yes	Yes	Yes
VM Plugin Support			
	No	Yes	Yes
Web Element Manager			
	Yes	Yes	Yes
Zoning			
Member selection	Yes	Yes	Yes
Zone editing	Yes	Yes	Yes
Live fabric library scope	Yes	Yes	Yes
QoS support	Yes	Yes	Yes
Zone alias support	Yes	Yes	Yes
Delete Zone database	No	Yes	Yes
Impact analysis	Yes	Yes	Yes
Remove offline devices	No	Yes	Yes
TI Zones	Yes	Yes	Yes
Device to Zone / zoneset participation analysis	Yes	Yes	Yes
LSAN Zones	No	Yes	Yes
Rolling back to an activated zone database	No	Yes	Yes
Import or export a zone database	No	Yes	Yes

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 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 is immediately logged out because the Product cannot reach the Server or Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

NOTE

Professional edition does not support remote clients.

Table 18 lists the default port numbers and whether or not it needs to be opened up in the firewall and 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.

TABLE 18 Port usage and firewall requirements

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
20 ¹	FTP Port (Control)	TCP	FTP Control port for internal FTP server	Client-Server Product-Server	Yes
21 ¹	FTP Port (Data)	TCP	FTP Data port for internal FTP server	Client-Server Product-Server	Yes
22 ²	SSH or 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/client to product	Server-Product Client-Product	Yes
25 ²	SMTP Server port	TCP	SMTP Server port for e-mail communication if you use e-mail notifications without SSL	Server-SMTP Server	Yes
49 ²	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

TABLE 18 Port usage and firewall requirements (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
80 ²	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 ¹	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 ²	SNMP port	UDP	Default SNMP port	Server-Product	Yes
162 ²	SNMP Trap port	UDP	Default SNMP trap port	Product-Server	Yes
389 ²	LDAP Authentication Server Port	UDP TCP	LDAP server port for authentication if you use LDAP as an external authentication	Server-LDAP Server	Yes
443 ^{1,2}	HTTPS server	TCP	HTTPS (HTTP over SSL) server port if you use secure client - server communication	Client-Server	Yes
443 ²			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 ²			HTTPS (HTTP over SSL) server port if you use vCenter discovery	Server-vCenter Server	Yes
465 ²	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 ²	Syslog Port	UDP	Default Syslog Port	Product-Server Managed Host - Server	Yes
636 ²	LDAP Authentication SSL port	TCP	LDAP server port for authentication if you use LDAP as an external authentication and SSL is enabled	Server-LDAP Server	Yes

A Management server and client ports

TABLE 18 Port usage and firewall requirements (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
1812 ²	RADIUS Authentication Server Port	UDP	RADIUS server port for authentication if you use RADIUS as an external authentication	Server-RADIUS Server	Yes
1813 ²	RADIUS Accounting Server Port	UDP	RADIUS server port for accounting if you use RADIUS as an external authentication	Server-RADIUS Server	Yes
5432	Database port	TCP	Port used by database if you access the 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 Server-Managed Host	Yes Yes
5989 ^{1,2}	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 Server-Managed Host	Yes Yes
6343 ²	sFlow	UDP	Receives sFlow data from products if you are monitoring with sFlow	Product-Server	Yes
24600 ^{1,2}	JNP (Java Naming Protocol) port	TCP	Use for service location. Uses SSL for privacy.	Client-Server	Yes
24601 ^{1,2}	EJB (Enterprise Java Bean) connection port	TCP	Client requests to server. Uses SSL for privacy.	Client-Server	Yes
24602 ^{1,2}	HornetQ Netty port	TCP	Use for JMS (Java Message Service), async messages from server to client. Uses SSL for privacy.	Client-Server	Yes
24603 ^{1,2}	JMX RMI port	TCP	Use for JMS control. Uses SSL for privacy.	Client-Server	Yes
24604 ^{1,2}	RMI naming service port	TCP		Client-Server	Yes
24605 ^{1,2}	RMI/JRMP invoker port	TCP		Client-Server	Yes
24606 ^{1,2}	Event Handling CIM Indication listener port	TCP	Used for HBA management	Managed Host - Server	Yes
24607 ^{1,2}	HCM Proxy CIM Indication Listener port	TCP	Used for HBA management	Managed Host - Server	Yes
24608 ²	Reserved for future use	TCP	Not used	Client - Server	No
24609 ²	Reserved for future use	TCP	Not used	Client - Server	No
24610 ²	Reserved for future use	TCP	Not used	Client - Server	No

TABLE 18 Port usage and firewall requirements (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
24611 ²	JBoss Transaction Services Recovery Manager port	TCP	Not used remotely	Server	Yes
24612 ²	JBoss Transaction Status Manager port	TCP	Not used remotely	Server	Yes
24613 ²	JBoss Pooled invoker port	TCP	Not used remotely	Server	Yes
24614 ²	JBoss Socket invoker port	TCP	Not used remotely	Server	Yes
24615 ²	JBoss RMI dynamic class loading port	TCP	Web service port, not used remotely	Server	Yes
24616 ²	Apache JServ port	TCP	Proxys web server requests, not used remotely	Server	Yes
24617 ²	Remote Management application connector access port	TCP	Not used remotely	Server	Yes
34568	HCM Agent discovery port	TCP	Used for HBA management via JSON	Server - Managed Host	Yes
55556 ¹	Launch in Context (LIC) client hand shaking port	TCP	Client port used to check if a Management application client 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

1. Port does not need to be open in the firewall for Professional edition.
2. 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.

Scalability limits

The following tables summarize the scalability limits for support with Network Advisor.

[Table 19](#) summarizes the SAN scalability limits for support with Network Advisor Enterprise edition.

TABLE 19 Enterprise-supported limits by SAN size

	Small	Medium	Large
Number of Fabrics	8	16	36
Number of Switches and Access Gateways	40	90	200
Number of Switch Ports	2000	5000	9000
Number of Device Ports	5000	10000	20000
Performance Monitoring Polling	5 minutes	5 minutes	5 minutes

A Scalability limits

Table 20 summarizes the SAN scalability limits for support with Network Advisor Professional Plus edition.

TABLE 20 Professional Plus-supported limits by SAN size

Values	Limits
Number of Fabrics	36
Number of Domains	20
Number of Switch Ports	2560
Number of Device Ports	4096
Number of Access Gateways	20
Performance Monitoring Polling	5 minutes

Table 21 summarizes the SAN scalability limits for support with Network Advisor Professional edition.

TABLE 21 Professional-supported limits by SAN size

Values	Limits
Number of Fabrics	1
Number of Domains	10
Number of Switch Ports	1000
Number of Device Ports	1000
Number of Access Gateways	5
Performance Monitoring Polling	N/A