

Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.2(3)

Release Date: January 8, 2008

Part Number: OL-14116-04

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the “[Related Documentation](#)” section on page 35.



Note

Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

Contents

This document includes the following sections:

- [Introduction](#), page 2
- [Components Supported](#), page 2
- [Software Download Process](#), page 7
- [Upgrading Your Cisco MDS SAN-OS Software Image](#), page 10
- [Downgrading Your Cisco MDS SAN-OS Software Image](#), page 20
- [New Features in Cisco MDS SAN-OS Release 3.2\(3\)](#), page 23
- [Limitations and Restrictions](#), page 23
- [Caveats](#), page 23
- [Related Documentation](#), page 35
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#), page 37



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© <year> Cisco Systems, Inc. All rights reserved.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Introduction

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides industry-leading availability, scalability, security, and management, allowing you to deploy high performance storage-area networks with lowest total cost of ownership. Layering a rich set of intelligent features onto a high performance, protocol agnostic switch fabric, the Cisco MDS 9000 Family addresses the stringent requirements of large data center storage environments: uncompromising high availability, security, scalability, ease of management, and seamless integration of new technologies.

The Cisco MDS 9000 Family SAN-OS is the underlying system software that powers the Cisco MDS 9500 Series, 9200 Series, and 9100 Series multilayer switches. The Cisco SAN-OS provides intelligent networking features, such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

Components Supported

Table 1 lists the SAN-OS software part number and hardware components supported by the Cisco MDS 9000 Family.



Note

To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S2K9-3.2.3	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.2.3	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S2K9-3.2.3	MDS 9222 Supervisor/Fabric-2, SAN-OS software.	MDS 9200 Series only
	M92S1K9-3.2.3	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S2K9-3.2.3	MDS 9100 Supervisor/Fabric-2, SAN-OS software.	MDS 9100 Series only
	M91S1K9-3.2.3	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9100FIC1EK9	FICON license.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
License	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS-14/2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS-14/2 module.	MDS 9200 Series
	M9500EXT1AK9	SAN Extension over IP package for MSM-18/4 module or MSFM-18/4 FIPS module.	MDS 9500 Series
	M9200EXT1AK9	SAN Extension over IP package for MSM-18/4 module or MSFM-18/4 FIPS module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with SSM
	M9500SME1MK9	Cisco Storage Media Encryption package for MSM-18/4 module	MDS 9500 Series with MSM
	M9200SME1MK9	Cisco Storage Media Encryption package for MSM-18/4 module	MDS 9200 Series with MSM
	M9200SME1FK9	Cisco Storage Media Encryption package for fixed slot	MDS 9222i Switch only
	M95DMMS1K9	Data Mobility Manager (DMM)	MDS 9500 Series with SSM
	M92DMMS1K9	Data Mobility Manager (DMM)	MDS 9200 Series with SSM
	M95DMMTS1K9	Data Mobility Manager (DMM) for 180 days	MDS 9500 Series with SSM
	M92DMMTS1K9	Data Mobility Manager (DMM) for 180 days	MDS 9200 Series with SSM
	M9124PL8-4G	On-Demand Ports Activation License	MDS 9124 Switch
	M9134PL8-4G	On-Demand Ports Activation License	MDS 9134 Switch
	M9134PL2-10G	On-Demand Ports Activation License	MDS 9134 Switch
	HP-PL12-4G	On-Demand Ports Activation License	Cisco Fabric Switch for HP c-Class BladeSystem only
	IBM-PL10-4G	On-Demand Ports Activation License	Cisco Fabric Switch for IBM BladeCenter only

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	MDS 9513 director (13-slot modular chassis with 11 slots for switching modules, and 2 slots reserved for Supervisor 2 modules only—SFPs ¹ sold separately).	MDS 9513 Switch only
	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9509 Switch only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 Switch only
	DS-C9222i-K9	MDS 9222i Multiservice Modular Switch (includes 18 4-Gbps Fibre Channel ports and 4 Gigabit Ethernet IP storage services ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Service modules.)	MDS 9222i Switch only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 Switch only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A Switch only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i Switch only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 Switch only
	DS-C9124-K9	MDS 9124 fixed configuration (non-modular) multilayer fabric switch (includes 8 enabled ports; an on-demand ports activation license can enable 8 additional ports, up to 24 ports).	MDS 9124 Switch only
	DS-C9134-K9	MDS 9134 fixed configuration (non-modular) multilayer fabric switch (includes 24 enabled 4-Gbps ports; an on-demand ports activation license can enable 8 additional ports, up to 32 4-Gbps ports. An additional port activation license can enable 2 10-Gbps ports.).	MDS 9134 Switch only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 Switch only
	DS-HP-FC-K9	Cisco Fabric Switch for HP c-Class BladeSystem (includes sixteen internal and eight external active ports and four 4-Gb SFPs installed, or eight internal and four external active ports and two 4-Gb SFPs installed).	Cisco Fabric Switch for HP c-Class BladeSystem only
DS-IBM-FC-K9	Cisco Fabric Switch for IBM BladeCenter (includes fourteen internal and six external ports)	Cisco Fabric Switch for IBM BladeCenter only	

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
External crossbar module	DS-13SLT-FAB1	MDS 9513 crossbar fabric module.	MDS 9513 Switch only
Supervisor modules	DS-X9530-SF2-K9	MDS 9500 Supervisor-2, module.	MDS 9500 Series only
	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I module.	
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
	DS-X9112	MDS 9000 12-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9124	MDS 9000 24-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9148	MDS 9000 48-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage services module.	MDS 9500 Series and 9200 Series
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage services module.	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
	DS-X9304-18K9	18-port Fibre Channel/4-port Gigabit Ethernet Multiservice (MSM-18/4) module.	
	DS-X9304-18FK9	18-port Fibre Channel/4-port Gigabit Ethernet Multiservice FIPS (MSFM-18/4) module.	
Optics	DS-X2-FC10G-SR	X2/SC optics, 10-Gbps Fibre Channel for Short Reach.	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X2-FC10G-LR	X2/SC optics, 10-Gbps Fibre Channel for Long Reach.	
	DS-X2-FC10G-ER	X2/SC optics, 10-Gbps Fibre Channel for Extended Reach (40 km).	
	DS-X2-E10G-SR	X2/SC optics, 10-Gbps Ethernet for Short Reach	
	DS-X2-FC10G_CX4	X2/CX-4 optics, 10-Gbps Fibre Channel, copper	

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW	2-Gbps/1-Gbps Fibre Channel—short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW	2-Gbps/1-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-GE-T	1-Gbps Ethernet SFP.	
	DS-SFP-FC4G-SW	4-Gbps/2-Gbps/1-Gbps Fibre Channel—short wavelength SFP for DS-X91xx switching modules.	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-SFP-FC4G-MR	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 4 km.	
	DS-SFP-FC4G-LW	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 10 km.	
CWDM ²	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps/4-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexers.	
Power supplies	DS-CAC-6000W	6000-W AC power supply.	MDS 9513 only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-3000W	3000-W AC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-300W	300-W ³ AC power supply.	MDS 9100 Series only
CompactFlash	MEM-MDS-FLD51M	MDS 9500 supervisor CompactFlash disk, 512 MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family
CD-ROM	M90FMK9-CD322=	MDS 9000 Management Software and Documentation CD-ROM, spare.	MDS 9000 Family

1. SFP = small form-factor pluggable
2. CWDM = coarse wavelength division multiplexing
3. W = Watt

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Software Download Process

Use the software download procedure to upgrade to a later version, or downgrade to an earlier version, of an operating system. This section describes the software download process for the Cisco MDS SAN-OS and includes the following topics:

- [Determining the Software Version, page 7](#)
- [Downloading Software, page 7](#)
- [Selecting the Correct Software Image for an MDS 9200 Series Switch, page 8](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 9](#)
- [Configuring Generation 2 Switching Modules, page 9](#)

Determining the Software Version

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log in to the switch and enter the **show version EXEC** command.

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.



Note

We strongly recommend that you use the latest available software release supported by your vendor for all Cisco MDS 9000 Family products.

Downloading Software

The Cisco MDS SAN-OS software is designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

To download the latest Cisco MDS SAN-OS software, access the Software Center at this URL:

<http://www.cisco.com/public/sw-center>

See the following sections in this release note for details on how you can nondisruptively upgrade your Cisco MDS 9000 switch. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade, enables the compatibility check. The check indicates if the upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch and the reason.

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	rolling	
2	yes	disruptive	rolling	Hitless upgrade is not supported
3	yes	disruptive	rolling	Hitless upgrade is not supported
4	yes	non-disruptive	rolling	
5	yes	non-disruptive	reset	
6	yes	non-disruptive	reset	

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:1.3(x)_filename** command determines which additional features need to be disabled.

Send documentation comments to mdsfeedback-doc@cisco.com



Note

Refer to the “Determining Software Compatibility” section of the *Cisco MDS 9000 Family CLI Configuration Guide* for more details.



Note

If you would like to request a copy of the source code under the terms of either GPL or LGPL, please send an e-mail to mds-software-disclosure@cisco.com.

Selecting the Correct Software Image for an MDS 9100 Series Switch

The system and kickstart image that you use for an MDS 9100 series switch depends on which switch you use, as shown in [Table 2](#).

Table 2 *Software Images for MDS 9100 Series Switch*

Switch	Image
MDS 9120 or MDS 9140	Filename begins with m9100-s1ek9
MDS 9134, MDS 9124, Cisco Fabric Switch for HP BladeSystem, or Cisco Fabric Switch for IBM BladeCenter	Filename begins with m9100-s2ek9

Selecting the Correct Software Image for an MDS 9200 Series Switch

The system and kickstart image that you use for an MDS 9200 series switch depends on which switch you use, as shown in [Table 3](#).

Table 3 *Software Images for MDS 9200 Series Switches*

Switch	Image
MDS 9222i	Filename begins with m9200-s2ek9
MDS 9216A or MDS 9216i	Filename begins with m9200-ek9

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series switch depends on whether the switch is based on a Supervisor-1 module or a Supervisor-2 module, as shown in [Table 4](#).

Table 4 *Software Images for Supervisor Type*

Supervisor Type	Switch	Image
Supervisor-1 module	MDS 9506 and 9509	Filename begins with m9500-sf1ek9
Supervisor-2 module	MDS 9506, 9509, and 9513	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch. For a Supervisor-1 module, the output might look like this:

Send documentation comments to mdsfeedback-doc@cisco.com

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---
...
...
5    0      Supervisor/Fabric-1       DS-X9530-SF1-K9     active*
6    0      Supervisor/Fabric-1       DS-X9530-SF1-K9     ha-standby
```

For a Supervisor-2 module, the output might look like this:

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---
...
...
7    0      Supervisor/Fabric-2       DS-X9530-SF2-K9     active *
8    0      Supervisor/Fabric-2       DS-X9530-SF2-K9     ha-standby
```

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

As of Cisco MDS SAN-OS Release 3.0(1), the Cisco MDS 9509 and 9506 Directors support both Supervisor-1 and Supervisor-2 modules. Supervisor-1 and Supervisor-2 modules cannot be installed in the same switch, except during migration. Both the active and standby supervisor modules must be of the same type, either Supervisor-1 or Supervisor-2 modules. For Cisco MDS 9513 Directors, both supervisor modules must be Supervisor-2 modules.



Caution

Migrating your supervisor modules is a disruptive operation.



Note

Migrating from Supervisor-2 modules to Supervisor-1 modules is not supported.

To migrate from a Supervisor-1 module to a Supervisor-2 module, refer to the step-by-step instructions in the [Cisco MDS 9000 Family CLI Configuration Guide](#).

Configuring Generation 2 Switching Modules

The Cisco MDS 9500 Multilayer Directors are designed to operate with any combination of Cisco MDS 9000 Generation 1 and Generation 2 modules. However, there are limitations to consider when combining the various modules and supervisors in the Cisco MDS 9500 Series platform chassis. The references listed in this section provide specific information about configurations that combine different modules and supervisors.

For information on configuring Generation 2 switching modules, refer to:

http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664c6b.html

For information on port index availability, refer to:

http://www.cisco.com/en/US/products/ps5990/products_installation_guide_chapter09186a0080419599.html

For information on Cisco MDS 9000 hardware and software compatibility, refer to:

http://www.cisco.com/en/US/products/ps5989/products_device_support_table09186a00805037ee.html

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Upgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for upgrading your Cisco MDS SAN-OS software image and contains the following sections:

- [Upgrading Your Version of Cisco Fabric Manager, page 10](#)
- [Upgrading with IVR Enabled, page 15](#)
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(3\), page 17](#)
- [Upgrading the SSI Image on Your SSM, page 18](#)
- [Upgrading a Switch with Insufficient Space for Two Images on the Bootflash, page 18](#)
- [Upgrading a Cisco MDS 9124 Switch, page 19](#)
- [Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch, page 19](#)

Upgrading Your Version of Cisco Fabric Manager

As of Cisco SAN-OS Release 3.2(1), Cisco Fabric Manager is no longer packaged with a Cisco MDS 9000 Family switch. It is included on the CD-ROM that ships with the switch. You can install Fabric Manager from the CD-ROM or from files that you download.

Installing Cisco Fabric Manager is a multi-step process that involves installing a database, as well as Fabric Manager. The complete installation instructions are provided in the “Installation of Cisco MDS SAN-OS and Fabric Manager” section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, and are available on-screen once you launch the Fabric Manager installer from the CD-ROM.

The following section presents the flow of the installation process at a high level. Review these guidelines before you begin the installation process.

1. Verify supported software. Cisco Fabric Manager has been tested with the following software:
 - Windows 2000 SP4, 2003 SP2, XP SP2
 - Redhat Linux (2.6 Kernel)
 - Solaris (SPARC) 8 and 10
 - VMWare Server 1.0:
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows XP SP2
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows 2000 SP4
 - Java Sun JRE and JDK 1.5(x) are supported
 - Java Web Start 1.2, 1.0.1, and 1.5
 - Firefox 1.5 and 2.0
 - Internet Explorer 6.x, and 7.0



Note Internet Explorer 7.0 is not supported on Windows 2000 SP4.

- Oracle Database 10g Express
- PostgreSQL 8.2 (Windows and Linux)
- PostgreSQL 8.1 (Solaris)

Send documentation comments to mdsfeedback-doc@cisco.com

- Cisco ACS 3.1 and 4.0
 - PIX Firewall
 - IP Tables
 - SSH v2
 - Global Enforce SNMP Privacy Encryption
 - HTTPS
2. Ensure data migration when upgrading Cisco Fabric Manager from Cisco SAN-OS Releases 3.1(2b) and later.

If you are upgrading Cisco Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and later, be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle Database 10g Express to Oracle Database 10g Express. If you migrate the database from Oracle to Oracle, the schema is updated.

3. Ensure data migration when upgrading Cisco Fabric Manager from releases prior to Cisco SAN-OS Releases 3.1(2b).

If you are upgrading Fabric Manager in a Cisco SAN-OS Release prior to 3.1(2b), be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or the Oracle Database 10g Express during the installation. The Fabric Manager Installer installs the PostgreSQL database on Windows. If you want to install the PostgreSQL database on Solaris or Linux, or if you want to install the Oracle Database 10g Express database, follow the instructions in the “Installation of Cisco MDS SAN-OS and Fabric Manager” section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.



Note If you are upgrading a previous installation of Fabric Manager, make sure the previous installation is installed and running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved.

4. Select the database.

If you want to use the Oracle Database 10g Express, you must install the database and create a user name and password before continuing with the Fabric Manager installation. We recommend the Oracle Database 10g Express option for all users who are running Performance Manager on large fabrics (1000 or more end devices).

If you want to install the PostgreSQL database, you must disable any security software you are running as PostgreSQL may not install certain folders or users. You must also log in as a Superuser before you start the installation.
5. Install Fabric Manager from the CD-ROM or from files that you download from Cisco.com at the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

To install Fabric Manager on Solaris, follow these steps:

-
- Step 1** Set Java 1.5 to the path that is to be used for installing Fabric Manager.
 - Step 2** Install the database that is to be used with Fabric Manager.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 3** Copy the Fabric Manager jar file **m9000-fm-3.2.3.jar** from the CD-ROM to a folder on the Solaris workstation.
- Step 4** Launch the installer using the following command:
- ```
java -Xms512m -Xmx512m -jar m9000-fm-3.2.3.jar
```
- Step 5** Follow the onscreen instructions provided in the Fabric Manager management software setup wizard.

To install Fabric Manager on Windows, follow these steps:

- Step 1** Click the **Install Management Software** link.
- Step 2** Choose **Management Software > Cisco Fabric Manager**.
- Step 3** Click the **Installing Fabric Manager** link.
- Step 4** Select the drive for your CD-ROM.
- Step 5** Click the **FM Installer** link.
- Step 6** Follow the onscreen instructions provided in the Fabric Manager Installer 3.2(3).

To install Device Manager on your workstation, follow these steps:

- Step 1** Enter the IP address of the switch in the Address field of your browser.
- Step 2** Click the **Cisco Device Manager** link in the Device Manager installation window.
- Step 3** Click **Next** to begin the installation.
- Step 4** Follow the onscreen instructions to complete the installation of Device Manager.



### Note

If you use a Java JDK instead of a JRE on Solaris, you might encounter a problem trying to install the Device Manager from a web browser. This can happen because the installer heap limit of 256 MB is not sufficient. If you have this problem, save the `jnlp` link as file, increase the heap limit to 512 MB, and run `javaws element-manager.jnlp` at the shell prompt.

## General Upgrading Guidelines

Use the following guidelines when upgrading to Cisco MDS SAN-OS Release 3.2(3):

- Install and configure dual supervisor modules.
- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- Follow the recommended guidelines for upgrading a Cisco MDS 9124 Switch as described in [“Upgrading a Cisco MDS 9124 Switch” section on page 19](#).
- Follow the guidelines for upgrading a single supervisor switch as described in [“Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch” section on page 19](#).
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively upgraded. See [Table 5](#) for the nondisruptive upgrade path for all SAN-OS releases.
- **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.
- **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
- **Inter-VSAN Routing (IVR):** With IVR enabled, you must follow additional steps if you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the “[Upgrading with IVR Enabled](#)” section on page 15 for these instructions.
- **FICON:** If you have FICON enabled, the upgrade path is different. See [Table 6](#).

Use [Table 5](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.2(3). Find the image release number you are currently using in the Current column of the table and use the path recommended.



**Note**

The software upgrade information in [Table 5](#) applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

**Table 5 Nondisruptive Upgrade Path to SAN-OS Release 3.2(3)**

| Current        | Nondisruptive Upgrade Path                                         |
|----------------|--------------------------------------------------------------------|
| SAN-OS 3.2(2c) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.2(1a) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(4)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(3a) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(2b) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(2a) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(2)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.1(1)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(3a) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(3)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(2a) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(2)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(1)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 2.1(3)  | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 2.1(2e) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 2.1(2d) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 2.1(2b) | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 5 Nondisruptive Upgrade Path to SAN-OS Release 3.2(3) (continued)**

| <b>Current</b> | <b>Nondisruptive Upgrade Path</b>                                                                                                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SAN-OS 2.1(2)  | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(3). |
| SAN-OS 2.1(1b) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(3). |
| SAN-OS 2.1(1a) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(3). |
| SAN-OS 2.0(x)  | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(3). |
| SAN-OS 1.x     | Upgrade to SAN-OS Release 1.3(4a), then to Release 2.1(2b), and then upgrade to Release 3.2(3).                                                                                                                                                                                                                   |

Use [Table 6](#) to determine your FICON nondisruptive upgrade path to Cisco MDS SAN-OS Release 3.2(3). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.

**Table 6 FICON Nondisruptive Upgrade Path to SAN-OS 3.2(3)**

| <b>Current Release with FICON Enabled</b> | <b>Upgrade Path</b>                                                |
|-------------------------------------------|--------------------------------------------------------------------|
| SAN-OS 3.0(3b)                            | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |
| SAN-OS 3.0(2)                             | You can nondisruptively upgrade directly to SAN-OS Release 3.2(3). |

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 6 FICON Nondisruptive Upgrade Path to SAN-OS 3.2(3)**

| Current Release with FICON Enabled | Upgrade Path                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SAN-OS 2.0(2b)                     | Use the <b>interface shutdown</b> command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively upgrading from SAN-OS Release 2.0(2b) to SAN-OS Release 3.0(2) or SAN-OS Release 3.0(3b), and then upgrade to Release 3.2(3). An operationally down state includes <code>Link failure or not-connected</code> , <code>SFP not present</code> , or <code>Error Disabled</code> status in the output of a <b>show interface</b> command. When an interface is administratively shut it will then show as <code>Administratively down</code> . Interfaces that are currently up or trunking do not need to be shut down. |
| SAN-OS 1.x                         | Upgrade to SAN-OS Release 3.0(2). Use the <b>interface shutdown</b> command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively upgrading to Release 2.0(2b) and then upgrade to 1.3(4a).                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Upgrading with IVR Enabled

An Inter-Switch Link (ISL) flap resulting in fabric segmentation or a merge during or after an upgrade from Cisco MDS SAN-OS Release 2.0(x) to a later image where IVR is enabled might be disruptive. Some possible scenarios include the following:

- FCIP connection flapping during the upgrade process resulting in fabric segmentation or merge.
- ISL flap results in fabric segmentation or merge because of hardware issues or a software bug.
- ISL port becomes part of PCP results in fabric segmentation or merge because of a port flap.

If this problem occurs, syslog messages indicate a failure and the flapped ISL could remain in a down state because of a domain overlap.

This issue was resolved in Cisco SAN-OS Release 2.1(2b); you must upgrade to Release 2.1(2b) before upgrading to Release 3.2(3). An upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) when IVR is enabled requires that you follow the procedure below, and then follow the upgrade guidelines listed in the [“Upgrading Your Version of Cisco Fabric Manager”](#) section on page 10. If you have VSANs in interop mode 2 or 3, you must issue an IVR refresh for those VSANs.

To upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) for all other VSANs with IVR enabled, follow these steps:

- Step 1** Configure static domains for all switches in all VSANs where IVR is enabled. Configure the static domain the same as the running domain so that there is no change in domain IDs. Make sure that all domains are unique across all of the IVR VSANs. We recommend this step as a best practice for IVR-non-NAT mode. Issue the **fcdomain domain id static vsan vsan id** command to configure the static domains.



**Note** Complete Step 1 for all switches before moving to Step 2.

- Step 2** Issue the **no ivr virtual-fc-domain-add vsan-ranges vsan-range** command to disable RDI mode on all IVR enabled switches. The range of values for a VSAN ID is 1 to 4093. This can cause traffic disruption.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**



---

**Note** Complete Step 2 for all IVR enabled switches before moving to Step 3.

---

**Step 3** Check the syslogs for any ISL that was isolated.

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
port-channel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface port-channel 51
(reason: domain ID assignment failure)
```

**Step 4** Issue the following commands for the isolated switches in Step 3:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan vsan-id suspend
switch(config-vsan-db)# no vsan vsan-id suspend
```

**Step 5** Issue the **ivr refresh** command to perform an IVR refresh on all the IVR enabled switches.

**Step 6** Issue the **copy running-config startup-config** command to save the RDI mode in the startup configuration on all of the switches.

**Step 7** Follow the normal upgrade guidelines for Release 2.1(2b). If you are adding new switches running Cisco MDS SAN-OS Release 2.1(2b) or later, upgrade all of your existing switches to Cisco SAN-OS Release 2.1(2b) as described in this workaround. Then follow the normal upgrade guidelines for Release 3.2(3).



---

**Note** RDI mode should not be disabled for VSANs running in interop mode 2 or interop mode 3.

---



[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

## Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2(3)

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode, which is the default for releases prior to Release 3.0(1).



### Note

To avoid any traffic disruption, modify the configuration of the SSM ports as described below, before upgrading a SAN-OS software image prior to Release 3.2(3).

For more information on upgrading SAN-OS software, see the [“Upgrading Your Cisco MDS SAN-OS Software Image” section on page 10](#).

If the configuration is not updated before the upgrade, the installation process for the new image will automatically convert all ports configured in auto mode to Fx mode. This change in mode might cause a disruption if the port is currently operating in E mode.

To upgrade the image on your SSM without any traffic disruption, follow these steps:

**Step 1** Verify the operational mode for each port on the SSM using the **show interface** command:

```
switch# show interface fc 2/1 - 32
fc2/1 is up
 Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
 Port WWN is 20:4b:00:0d:ec:09:3c:00
 Admin port mode is auto <----- shows port is configured in auto mode
 snmp traps are enabled
 Port mode is F, FCID is 0xef0300 <----- shows current port operational mode is F
 Port vsan is 1
 Speed is 2 Gbps
 Transmit B2B Credit is 3
```

**Step 2** Change the configuration for the first port of the quad when the admin port mode is auto. (A quad is a group of four ports, supported by a data path processor (DPP). The groups are 1 to 4, 5 to 8, 9 to 12, and so on.) Do not leave the port mode set to auto.

- a. Set the port admin mode to E or Fx if the current operational port mode is E, TE, F or FL.

```
switch# config t
switch(config)# interface fc 2/1
switch(config-if)# switchport mode fx
```

- b. Set the port admin mode to E if the current operational port mode is E:

```
switch# config t
switch(config)# interface fc 2/5
switch(config-if)# switchport mode e
```

**Step 3** Change the configuration for ports 2, 3, and 4 of the quad:

- a. Set the admin port mode to Fx if the admin port mode of these ports is E, TE, or auto.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# switchport mode fx
```

- b. If the first port in the port group has admin mode E or if the port is operational in E port mode, change the admin state of ports 2, 3, and 4 to shutdown.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# shutdown
```

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- Step 4** Save the running configuration to the startup configuration before the upgrade procedure to ensure that the changes are preserved during and after the upgrade. To save the configuration, enter the following command:

```
switch# copy running-config startup-config
```

## Upgrading the SSI Image on Your SSM

Use the following guidelines to nondisruptively upgrade the SSI image on your SSM:

- Install and configure dual supervisor modules.
- SSM intelligent services traffic on SSM ports is disrupted during upgrades. Fibre Channel switching traffic is not disrupted under the following conditions:
  - Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the [Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images](#).
  - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine what applications are configured. Use the **no ssm enable feature** CLI command to disable these applications.
  - No SSM ports are in auto mode. See the “[Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(3\)](#)” section on page 17.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** CLI command to determine your EPLD version. Refer to the [Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images](#) to upgrade your EPLD image.
  - Refer to the [Cisco MDS Storage Services Module Interoperability Support Matrix](#) and the “[Managing Modules](#)” chapter in the [Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x](#), for information on upgrading your SSM.



### Caution

Upgrading from Cisco MDS SAN-OS Release 2.1(1b) or earlier to Release 2.1.2 or later can disrupt traffic on any SSM installed on your MDS switch

## Upgrading a Switch with Insufficient Space for Two Images on the Bootflash

To upgrade the SAN-OS image on a Cisco MDS 9000 Family switch requires enough space on the internal CompactFlash (also referred to as bootflash) to accommodate both the old software image and the new software image.


As of Cisco MDS SAN-OS Release 3.1(1), on MDS switches with a 256-MB CompactFlash, it is possible in some scenarios that a user might be unable to fit two images on the bootflash. This lack of space on the bootflash might cause the upgrade process to fail because new images are always copied onto the bootflash during an upgrade.

The following MDS switches are affected by this issue:

- MDS 9216 and MDS 9216i
- MDS 9120 and MDS 9140
- MDS 9500 Series switches with a Supervisor 1 module

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

To work around an image upgrade failure caused by a lack of space on the bootflash, follow these steps:

- 
- Step 1** Prior to installing the new image, copy the old (existing) system image file to an external server. You may need to reinstall this file later.
- Step 2** Delete the old system image file from the bootflash by using either the Fabric Manager install utility or the CLI **delete bootflash:** command. The system image file does not contain the word “kickstart” in the filename.
- ```
switch# delete bootflash:m9200-ek9-mz.3.0.3.bin
```
-
-  **Note** On MDS 9500 Series switches, you also need to delete the image file from the standby supervisor after deleting it from the active supervisor.
- ```
switch# delete bootflash://sup-standby/m9500-sf1ek9-mz.3.0.3.bin
```
- 
- Step 3** Start the image upgrade or installation process using the Fabric Manager install utility or the CLI **install all** command.
- Step 4** If the new installation or upgrade fails while copying the image and you want to keep the old (existing) image, then copy the old image (that you saved to an external server in Step 1) to the bootflash using either Fabric Manager or the **copy** command.
- Step 5** If the switch fails to boot, then follow the recovery procedure described in the “Troubleshooting Installs, Upgrades, and Reboots” section of the *Cisco MDS 9000 Family Troubleshooting Guide, Release 3.x*.

## Upgrading a Cisco MDS 9124 Switch

If you are upgrading from Cisco MDS SAN-OS Release 3.1(1) to Cisco SAN-OS Release 3.2(3) on a Cisco MDS 9124 Switch, follow these guidelines:

- During the upgrade, configuration is not allowed and the fabric is expected to be stable.
- The Fabric Shortest Path First (FSPF) timers must be configured to the default value of 20 seconds; otherwise, the nondisruptive upgrade is blocked to ensure that the maximum down time for the control plane can be 80 seconds.
- If there are any CFS commits in the fabric, the nondisruptive upgrade will fail.
- If there is a zone server merge in progress in the fabric, the nondisruptive upgrade will fail.
- If a service terminates the nondisruptive upgrade, the **show install all failure-reason** command can display the reason that the nondisruptive upgrade cannot proceed.
- If there is not enough memory in the system to load the new images, the upgrade will be made disruptive due to insufficient resources and the user will be notified in the compatibility table.

## Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

Cisco MDS SAN-OS software upgrades are disruptive on the following single supervisor Cisco MDS Family switches:

- MDS 9120 switch
- MDS 9140 switch
- MDS 9216i switch

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path shown in [Table 5](#), even though the upgrade is disruptive. Following the nondisruptive upgrade path ensures that the binary startup configuration remains intact.

If you do not follow the upgrade path, (for example, you upgrade directly from SAN-OS Release 2.1(2) or earlier version to SAN-OS Release 3.2(3)), the binary startup configuration is deleted because it is not compatible with the new image, and the ASCII startup configuration file is applied when the switch comes up with the new upgraded image. When the ASCII startup configuration file is applied, there may be errors. Because of this, we recommend that you follow the nondisruptive upgrade path.

## Downgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for downgrading your Cisco MDS SAN-OS software image and contains the following sections:

- [General Downgrading Guidelines, page 20](#)
- [Downgrading the SSI Image on Your SSM, page 22](#)

### General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.2(3):

- Install and configure dual supervisor modules.
- Issue the system **no acl-adjacency-sharing** execute command to disable acl adjacency usage on Generation 2 and Generation 1 modules. If this command fails, reduce the number of zones, IVR zones, TE ports, or a combination of these in the system and issue the command again.
- Disable all features not supported by the downgrade release. Use the **show incompatibility system downgrade-image** CLI command to determine what you need to disable.
- Layer 2 switching traffic is not disrupted when downgrading to Cisco SAN-OS Release 2.1(2) or later.
- Use the **show install all impact downgrade-image** CLI command to determine if your downgrade will be nondisruptive.
- Be aware that some features impact whether a downgrade is disruptive or nondisruptive:
  - **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively downgraded. See [Table 7](#) for the nondisruptive downgrade path for all SAN-OS releases.
  - **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during a downgrade. SSM Fibre Channel traffic is not.
  - **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the downgrade is in progress.
  - **iSCSI:** If you are downgrading from SAN-OS version 3.0(x) to a lower version of SAN-OS, enable iSCSI if an IPS module, MPS-14/2 module, MSM-18/4 module, or the MDS 9222i switch is online. Otherwise, the downgrade will disrupt traffic.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- **IVR:** With IVR enabled, you must follow additional steps if you are downgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the “[Upgrading with IVR Enabled](#)” section on page 15 for these instructions.
- **FICON:** If you have FICON enabled, the downgrade path is different. See [Table 8](#).

Use [Table 7](#) to determine the nondisruptive downgrade path from Cisco SAN-OS Release 3.2(3). Find the SAN-OS image you want to downgrade to in the To SAN-OS Release column of the table and use the path recommended.



**Note**

The software downgrade information in [Table 7](#) applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

**Table 7 Nondisruptive Downgrade Path from SAN-OS Release 3.2(3)**

| To SAN-OS Release | Nondisruptive Downgrade Path                                                                                    |
|-------------------|-----------------------------------------------------------------------------------------------------------------|
| SAN-OS 3.2(2c)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.2(1a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1(4)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1(3a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1(2b)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1        | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1(2)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.1(1)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.0(3a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.0(3)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.0(2a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.0(2)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 3.0(1)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 2.1(3)     | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 2.1(2e)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 2.1(2d)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 2.1(2b)    | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                          |
| SAN-OS 2.1(2)     | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(2).                                       |
| SAN-OS 2.1(1b)    | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(1b).                                      |
| SAN-OS 2.1(1a)    | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(1a).                                      |
| SAN-OS 2.0(4a)    | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(4a).                                      |
| SAN-OS 2.0(4)     | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(4).                                       |
| SAN-OS 2.0(3)     | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(3).                                       |
| SAN-OS 2.0(2b)    | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(2b).                                      |
| SAN-OS 2.0(1b)    | Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(1b).                                      |
| SAN-OS 1.x        | Downgrade to SAN-OS to Release 2.1(2b), then to Release 1.3(4a), and then downgrade to your SAN-OS 1.x release. |

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Use [Table 8](#) to determine your nondisruptive downgrade path, if you have FICON enabled, from Cisco SAN-OS Release 3.2(3). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.

**Table 8** FICON Downgrade Path from SAN-OS 3.2(3)

| To SAN-OS Release with FICON Enabled | Downgrade Path                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SAN-OS 3.0(3b)                       | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SAN-OS 3.0(2)                        | You can nondisruptively downgrade directly from SAN-OS Release 3.2(3).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SAN-OS 2.0(2b)                       | Use the <b>interface shutdown</b> command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively downgrading from SAN-OS Release 3.2(3) to SAN-OS Release 3.0(3b) or SAN-OS Release 3.0(2), and then to SAN-OS Release 2.0(2b). An operationally down state includes <code>Link failure</code> or <code>not-connected</code> , <code>SFP not present</code> , or <code>Error Disabled</code> status in the output of a <b>show interface</b> command. When an interface is administratively shut it will then show as <code>Administratively down</code> . Interfaces that are currently up or trunking do not need to be shut down. |
| SAN-OS 1.3(4a)                       | Downgrade to SAN-OS Release 3.0(2). Use the shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively downgrading to Release 2.0(2b) and then downgrade to 1.3(4a).                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Downgrading the SSI Image on Your SSM

Use the following guidelines when downgrading your SSI image on your SSM.

- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco SAN-OS Release 3.2(3) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the [Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images](#).
- SSM intelligent services traffic switching on SSM ports is disrupted on upgrades or downgrades.
- Fibre Channel switching traffic on SSM ports is not disrupted under the following conditions:
  - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode CLI command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** CLI command to determine your EPLD version. Refer to the [Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images](#) to upgrade your EPLD image.
  - Refer to the [Cisco MDS Storage Services Module Interoperability Support Matrix](#) and to the “Managing Modules” chapter in the [Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x](#) for information on downgrading your SSM.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## New Features in Cisco MDS SAN-OS Release 3.2(3)

This section briefly describes the new features introduced in this release. For detailed information about the features listed, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*, the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, and the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*. For information about new CLI commands associated with these features, refer to the *Cisco MDS 9000 Family Command Reference*. The “New and Changed Information” section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.



### Note

These release notes are specific to this release. For the complete Release 3.x documentation set, see the “[Related Documentation](#)” section.

There are no new features available for this release.

## Limitations and Restrictions

There are no limitations or restrictions for this release.

## Caveats

This section lists the open and resolved caveats for this release. Use [Table 9](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

**Table 9**      **Open Caveats and Resolved Caveats Reference**

| DDTS Number                  | Software Release (Open or Resolved) |        |
|------------------------------|-------------------------------------|--------|
|                              | 3.2(2c)                             | 3.2(3) |
| <b>Severity 2</b>            |                                     |        |
| • <a href="#">CSCsg17743</a> | O                                   | R      |
| • <a href="#">CSCsg49151</a> | O                                   | O      |
| • <a href="#">CSCsi62114</a> | O                                   | R      |
| • <a href="#">CSCsi72048</a> | O                                   | O      |
| • <a href="#">CSCsk43922</a> | O                                   | O      |
| • <a href="#">CSCsk49029</a> | O                                   | O      |
| • <a href="#">CSCsk49634</a> | O                                   | O      |
| • <a href="#">CSCsk49761</a> | O                                   | O      |
| • <a href="#">CSCsk51193</a> | O                                   | O      |
| • <a href="#">CSCsk54591</a> | O                                   | O      |
| • <a href="#">CSCsl24773</a> | O                                   | R      |
| • <a href="#">CSCsl28481</a> | O                                   | R      |

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 9 Open Caveats and Resolved Caveats Reference (continued)**

| DDTS Number       | Software Release (Open or Resolved) |        |
|-------------------|-------------------------------------|--------|
|                   | 3.2(2c)                             | 3.2(3) |
| •CSCsI39215       | O                                   | O      |
| •CSCsI53000       | O                                   | R      |
| •CSCsI58537       | O                                   | R      |
| •CSCsI65880       | O                                   | R      |
| •CSCsI65911       | O                                   | R      |
| •CSCsI66072       | O                                   | R      |
| •CSCsI71227       | O                                   | O      |
| •CSCsI65911       | O                                   | O      |
| •CSCsI75365       | O                                   | R      |
| <b>Severity 3</b> |                                     |        |
| •CSCin95789       | O                                   | O      |
| •CSCse31881       | O                                   | O      |
| •CSCse47687       | O                                   | O      |
| •CSCsg19148       | O                                   | O      |
| •CSCsg19303       | O                                   | O      |
| •CSCsi66310       | O                                   | O      |
| •CSCsj24904       | O                                   | O      |
| •CSCsj72666       | O                                   | O      |
| •CSCsk00953       | O                                   | O      |
| •CSCsk06186       | O                                   | O      |
| •CSCsk35725       | O                                   | O      |
| •CSCsk35951       | O                                   | O      |
| •CSCsk49309       | O                                   | O      |
| •CSCsk63929       | O                                   | O      |
| •CSCsk87502       | O                                   | O      |
| •CSCsk87614       | O                                   | O      |
| •CSCsk93834       | O                                   | O      |
| •CSCsk95241       | O                                   | O      |
| •CSCsI02669       | O                                   | R      |
| •CSCsI12130       | O                                   | O      |
| •CSCsI15511       | O                                   | O      |
| •CSCsI17944       | O                                   | O      |
| •CSCsI31087       | O                                   | O      |
| •CSCsI33763       | O                                   | O      |



**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 9** Open Caveats and Resolved Caveats Reference (continued)

| DDTS Number       | Software Release (Open or Resolved) |               |
|-------------------|-------------------------------------|---------------|
|                   | <b>3.2(2c)</b>                      | <b>3.2(3)</b> |
| •CSCs134922       | O                                   | O             |
| •CSCs141090       | O                                   | R             |
| •CSCs142923       | O                                   | R             |
| •CSCs149158       | O                                   | R             |
| •CSCs152998       | O                                   | R             |
| •CSCs160060       | O                                   | R             |
| •CSCs165913       | O                                   | R             |
| •CSCs165951       | O                                   | O             |
| <b>Severity 4</b> |                                     |               |
| •CSCsi56167       | O                                   | O             |
| •CSCsk91974       | O                                   | O             |
| •CSCs151357       | O                                   | R             |
| •CSCs155450       | O                                   | R             |
| <b>Severity 5</b> |                                     |               |
| •CSCsk73654       | O                                   | O             |
| <b>Severity 6</b> |                                     |               |
| •CSCsi43117       | O                                   | R             |
| •CSCsk43927       | O                                   | O             |
| •CSCsk90998       | O                                   | O             |
| •CSCsm13002       | O                                   | O             |
| •CSCsm15874       | O                                   | O             |
| •CSCsm17768       | O                                   | O             |
| •CSCsm18303       | O                                   | O             |

## Resolved Caveats

- CSCsg17743

**Symptom:** After a Supervisor switchover or after a standby Supervisor reload, the active Supervisor module is unable to communicate to the standby Supervisor and modules. This can result in the standby Supervisor not coming up or connection failures with modules.

**Workaround:** This issue is resolved.

- CSCsi62114

**Symptom:** An MDS 9513 switch running SAN-OS Release 3.1(2) my reload due to both Supervisors hitting a kernel within 6 seconds of each other. This does not occur when running SAN-OS Release 3.2(1a) or later.

**Workaround:** This issue is resolved.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- CSCs124773  
**Symptom:** If there are tape paths bound to the Cisco SME interface on an MDS 9222i switch, an upgrade on the MDS 9222i switch fails.  
**Workaround:** This issue is resolved.
- CSCs128481  
**Symptom:** Cisco SME is not supported on the HP VLS6100.  
**Workaround:** This issue is resolved.
- CSCs153000  
**Symptom:** In images prior to Release 3.2(3) on the Cisco 4 Gb Fibre Channel Switch Module for IBM BladeCenter, when NPV is enabled, the VPD chassis manager does not run on the switch. The following will occur:
  - The switch will not POST to the Management Module when booting.
  - The switch will not process any requests from the Management Module to disable external management or disable external ports.
  - If you try to change the switch IP address through the Management Module, the switch will become unresponsive and will require service.If NPV is not enabled, the switch will communicate correctly with the chassis Management Module.  
**Workaround:** This issue is resolved.
- CSCs165880  
**Symptom:** On the MDS 9222i switch, the internal communication channel between the data path processor and the module processor may fail after deleting or adding multiple tape devices in a cluster. This may cause the host to lose communication with the tapes.  
**Workaround:** This issue is resolved.
- CSCs165911  
**Symptom:** In rare instances, deleting tape devices corresponding to a target port from a Cisco SME configuration causes the host to lose connectivity to the tape drive for a long time.  
**Workaround:** This issue is resolved.
- CSCs166072  
**Symptom:** During a hitless upgrade from SAN-OS Release 3.0(x) (or lower) to Release 3.1(x) (or higher), and a subsequent switchover or hitless upgrade, under certain runtime conditions, the Port-Channel Manager process (PCM) may terminate and potentially cause the switch to reboot. This issue occurs with MDS 95xx platforms only regardless of the supervisor version.  
**Workaround:** This issue is resolved.
- CSCs175365  
**Symptom:** Using the Fabric Manager Standalone version, the client stops after configuration changes are made.  
**Workaround:** This issue is resolved.
- CSCs102669  
**Symptom:** When an incorrect fabric identifier is assigned to a fabric during initial discovery, Performance Manager displays the wrong number of flows when fabrics are discovered at a later time.  
**Workaround:** This issue is resolved.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- CSCs141090  
**Symptom:** During an upgrade from SANOS Release 3.0(x) (or lower) to Release 3.2(1) (or higher), if you perform an SNMPWALK operation of the CISCO-ENTITY-SENSOR-MIB on the switch during the upgrade, the snmpd process may terminate resulting in the loss of the SNMP profile or similar consequences. In some cases, this may result in a switchover or a reboot.  
**Workaround:** This issue is resolved.
- CSCs142923  
**Symptom:** The VSAN filter summary stops polling.  
**Workaround:** This issue is resolved.
- CSCs149158  
**Symptom:** After a non-disruptive upgrade to SAN-OS's 3.0(1) thru Release 3.2(2c), traffic LEDs on Generation 2 Module (DS-X9704) do not blink.  
**Workaround:** This issue is resolved.
- CSCs152998  
**Symptom:** When the FCIP compression mode is set to mode2 or it is set to Auto and the maximum bandwidth configured for the FCIP profile is less than 155Mbps, in rare cases (depending on the data pattern), there can be an FCIP link flap and the "Port Software Failure" error message is displayed.  
**Workaround:** This issue is resolved.
- CSCs158537  
**Symptom:** The CIM server does not authorize requests after an average of 25,000 requests. An unauthorized error is displayed.  
**Workaround:** This issue is resolved.
- CSCs160060  
**SYMPTOM:** With a device alias defined on an MDS switch and CFS is enabled for the device alias, and Fabric Manager shows fabric.fcalias=false, Fabric Manager does not populate the device alias to the host and target port table. A server discovery output shows a valid MDS switch as a device alias seed but there is no device alias.  

The device alias database checksum persists in the Fabric Manager database, but the alias has not persisted yet, the fabric is closed or unmanaged. When the fabric is loaded and managed the next time and it is rediscovered, the checksum does not change so the rediscovering device alias is skipped.

**Workaround:** This issue is resolved.
- CSCs165913  
**Symptom:** Using Fabric Manager Release 3.2(2), if you have an enclosure that spans multiple fabrics and not all the fabrics are managed and you then use the Data Migration Wizard to create a job with that enclosure as the existing storage (selecting all ports listed in that enclosure), an error is displayed in the creation wizard.  
**Workaround:** This issue is resolved.
- CSCs151357  
**Symptom:** The Device Manager Summary tab does not show multiple pWWNs that are on the NPV interface.  
**Workaround:** This issue is resolved.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- CSCsI55450  
**Symptom:** The Fabric Manager Server GUI displays "Finished searching the table. The search item not found." This occurs when you select Inventory and then Zones to display the Member column, then click the Find icon (binoculars). In the resulting window, you type a word that is not on the first page and click 'find from start'. The main web page appears to refresh, but does not actually locate anything.  
 If you search for an item that is not on the first page, an error message displays "Finished searching the table. The Search item not found".  
**Workaround:** None.
- CSCsi43117  
**Symptom:** CFS merge information does not include SNMP support.  
**Workaround:** This will be included in a future Fabric Manager release.

## Open Caveats

- CSCsg49151  
**Symptom:** If you bring up more than one link at a time between two VSANs that have overlapping domains and at least one of the switches is SDV enabled, one link will become isolated. The other links will come up, even though the domains are overlapping. In addition, the SDV virtual domains will change, causing traffic disruption on all devices associated with their old value.  
**Workaround:** Bring up multiple links between two switches one at a time. Verify that the first link came up correctly before attempting to bring up the next link. If the first link fails to come up because of a domain ID overlap, resolve the domain conflict and then try again to bring up the links.
- CSCsi72048  
**Symptom:** FCIP links may fail on an MDS 9216i switch that has compression set to auto when the other end of the FCIP link is terminated by an IPS-8 module. You may see the following message in the logs:  

```
%IPS_SB_MGR-SLOT1-3-CRYPTO_FAILURE: Heartbeat failure in encryption engine (error 0x1)
%ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface GigabitEthernet1/1 is down (Port software failure)
%PORT-5-IF_DOWN_SOFTWARE_FAILURE: %$VSAN 1%$ Interface fcip99 is down (Port software failure)
```

**Workaround:** If both ends of an FCIP link are not on an MPS-14/2 module, do not use mode 1 and auto.
- CSCsk43922  
**Symptom:** A data path processor (DPP) might fail on an MDS switch running SSI Release 3.2(1) on the SSM. The failure occurs after several days of running traffic when a misbehaving target sends unexpected frames well after the response has already been received from the same target.  
**Workaround:** None.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- CSCsk49029

**Symptom:** If there is a request to export a domain while the same domain is being cleaned up, domain entries might not be programmed. As a result, communication between IVR devices might not occur.

**Workaround:** Because the the programming request was lost, the only way to retrigger the programming is to withdraw the domain and refresh IVR. Follow these steps:

1. Identify domains with problem using the **show ivr internal dep** command.

```
switch# show ivr internal dep
Internal information for DEP FSM

vsan domain nh status sync_status req i/f
101 0x61(97) 1001 ALL_DONE OXID|FCID_RW 0 [fc3/2]
102 0x62(98) 1002 ALL_DONE OXID|FCID_RW 0 [fc3/5]
1001 0x9e(158) 101 NONE OXID|FCID_RW 0 [fc2/16]
1002 0x98(152) 102 ALL_DONE OXID|FCID_RW 0 [fc9/10]
Number of DEP entries : 4
```

After waiting for a few minutes for IVR to stabilize, if the status column for the {vsan, domain} combination is NONE, then this problem has occurred the switch.

2. Withdraw the troubled domains using the **ivr withdraw domain domain vsan vsan-id** command.
3. Readvertise the withdrawn domains using the **ivr refresh** command.

- CSCsk49634

**Symptom:** In rare cases, an FCIP link might flap on a network with high latency and a consistently high loss rate.

**Workaround:** None.

- CSCsk49761

**Symptom:** When IVR exports a new virtual domain and multiple border switches export that virtual domain, some of the entries in the Fibre Channel name server (FCNS) database that correspond to this virtual domain may have partial entries where the port type contains a dash (-). This can then lead to a lack of IVR communication between these devices and other IVR devices.

**Workaround:** Use the **show ivr internal vdri vsan vsan-id domain domain** command to determine which border switch is exporting the virtual domain. Then on any of the border switches that is exporting the virtual domain, enter the following command for each device that has a partial FCNS entry:

```
switch(config)# ivr device pwn pwn fcns register vsan vsan-id
```

In this example, pWWN is the port pWWN of the device and vsan-id is the VSAN that contains the incomplete FCNS entries.

- CSCsk51193

**Symptom:** Following an upgrade to Cisco MDS SAN-OS Release 3.2(1) on a Cisco MDS 9124 switch, an interface is shown as up, but there is no FLOGI information for the port in the FLOGI database.

**Workaround:** Set the port mode to F.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- CSCsk54591
 

**Symptom:** In rare cases, if two or more catastrophic exceptions affecting the MDS arbiter occur in quick succession, it is possible that an MDS 9500 Series switch will completely reset.

**Workaround:** None.
- CSCsl39215
 

**Symptom:** The CIM server stops. This occurs after creating a subscription using the same filter and handler.

**Workaround:** Reload the switch.
- CSCsl71227
 

**Symptom:** Using Fabric Manager Release 3.2(2), if you have an enclosure with multiple ports and you then use the Data Migration Wizard to create a job with that enclosure as the existing storage but don't select all the storage ports in the enclosure, an error is displayed in the creation wizard.

**Workaround:** Put the ports you plan to use as the existing storage in the migration into a separate enclosure, and use that enclosure in the wizard selection.
- CSCsl73987
 

**Symptom:** In rare instances, when a SCSI I/O is in progress in Cisco SME and it is aborted by the host, the Cisco SME interface may fail and a reset may occur.

**Workaround:** This issue is resolved.
- CSCin95789
 

**Symptom:** When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.

**Workaround:** Check the logs to clarify that the correct interface has been selected.
- CSCse31881
 

**Symptom:** If there are IP over Fibre Channel (IPFC) interfaces configured on an SSM, you might experience issues if you downgrade from SAN-OS Release 3.x to Release 2.x.

**Workaround:** Before downgrading, remove the IPFC interface on the module and then recreate the IPFC interface after the downgrade is complete.
- CSCse47687
 

**Symptom:** If IP ACLs are applied to any IP Storage Gigabit Ethernet port, implicit deny does not take effect.

**Workaround:** Configure explicit deny on the port.
- CSCsg19148
 

**Symptom:** Time zone changes that are executed on an MDS switch do not take effect on the 12-port, 24-port, and 48 port 1-Gbps/2-Gbps/4-Gbps Fibre Channel modules, and on the 4-port 10-Gbps module. This issue occurs in SAN-OS Releases 3.0(1), 3.0(2), 3.0(2a), and 3.0(3).

Time zone changes that are executed on an MDS switch do not take effect on the 16-port or 32-port 1-Gbps/2-Gbps module, on the 4-port or 8-port Gigabit Ethernet IP services module, the MPS-14/2 module, and on the SSM. This issue occurs in SAN-OS Release 3.0(3).

This issue has no effect on functionality. However, debug messages and syslogs from the MDS switching modules have incorrect timestamps if the time zone is configured on an MDS switch.

**Workaround:** None.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- CSCsg19303  
**Symptom:** Graceful shutdowns of ISLs are not supported for IVR traffic.  
**Workaround:** Increase the FSPF cost on the link before it is shut down, so that traffic will flow through an alternate path.
- CSCsi66310  
**Symptom:** The management port on MDS switches supports one user-configured IPv6 address, but does not support autoconfiguration of an IPv6 address in Cisco SAN-OS Release 3.2(1).  
**Workaround:** None.
- CSCsj24904  
**Symptom:** On a Gigabit Ethernet interface on an MDS MSM-18/4 module, shut the interface before removing its IP address so that configuration changes on the interface can take effect. This applies only to the Gigabit Ethernet ports in slot 1 of the MDS 9222i switch and the MDS 9216i switch.  
**Workaround:** Always shut the interface using the **shutdown** command before removing the IP address and making configuration changes.
- CSCsj72666  
**Symptom:** In certain conditions, an MDS switch may not be able to determine the FC4-type of certain targets. This causes the targets to be listed in the hosts section during a Cisco SME tape group or tape device configuration.  
**Workaround:** Issue the **discover scsi-target vsan vsan-id fcid fcid** command to re-discover the FC4-type of the targets. A Cisco SME tape group or tape device configuration will now list the targets correctly.
- CSCsk00953  
**Symptom:** HP Blade Servers that are connected through an HP Virtual Connect (VC) FC module to a Cisco Fabric Switch for HP c-Class BladeSystem using NPIV lose access to LUNs when load balancing on the VC module is switched from 16:1 to 8:1. When the load balancing ratio is 16:1, all servers connect through interface ext1. When the ratio is 8:1, servers 1 and 3 connect through ext1, servers 2 and 4 connect through ext2, and so on. Servers on ext2 are not affected by the switchover. In addition, packets might get dropped when the switchover occurs.  
**Workaround:** None.
- CSCsk06186  
**Symptom:** In rare situations, on an MDS 9513 director switch, an upgrade fails when a standby supervisor does not come up to a state that the installer recognizes. As a result, the standby supervisor is reloaded to recover and the system runs the older configuration version.  
**Workaround:** Perform the upgrade again.
- CSCsk35725  
**Symptom:** Fabric Manager takes 2 to 3 minutes to bring up the DMM job creation wizard in a setup with 25 switches, 400 enclosures, and 2400 entries in the name server.  
**Workaround:** None.
- CSCsk35951  
**Symptom:** In a configuration with a PortChannel with FCIP members and write acceleration in use, if IVR NAT is enabled on one end of the PortChannel and not enabled on the other end, then traffic over the FCIP tunnel might fail.  
**Workaround:** Enable IVR NAT on both ends of the PortChannel or disable it on both ends.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- CSCsk49309  
**Symptom:** IPv6 duplicate address detection (DAD) may not always work for the management port.  
**Workaround:** None.
- CSCsk63929  
**Symptom:** If DMM is provisioned on the SSM and you downgrade to a Cisco MDS SAN-OS release that does not support DMM, the configuration persists and the GUI and CLI show DMM as a provisioned application.  
**Workaround:** Manually remove the DMM configuration from the switch before downgrading to a Cisco MDS SAN-OS release that does not support DMM, such as downgrading from SAN-OS Release 3.2(1) to SAN-OS Release 3.1(3). If you forget to remove the configuration before the downgrade, power off the module and purge the configuration on the SSM module by entering the following commands:  

```
switch(config)# poweroff module slot
switch# purge module slot running-config
```
- CSCsk87502  
**Symptom:** If an NASB configuration in a VSAN is destroyed while a target discovery is pending, the NASB process fails. Issue the **show nasb vsan x** command on the SSM to view the target discovery in the Pending state.  
**Workaround:** Reload the SSM.
- CSCsk87614  
**Symptom:** When NASB is enabled in a VSAN, all targets that are visible in that VSAN are discovered by NASB. If a new target is added to the VSAN, NASB does not automatically discover the new target.  
**Workaround:** To discover the new target, reload the SSM or disable and re-enable NASB in the VSAN.
- CSCsk93834  
**Symptom:** In rare situations during a storage-based online data migration job, the user might not be able to destroy the job if the following sequence of events occurs:
  1. A storage-based data migration job is executing.
  2. A port flap occurs on the server and the server HBA port goes down.
  3. The storage-based data migration job continues executing until it completes.
  4. The user issues the **dmm module module-id job job-id destroy** command to delete the storage-based data migration job, but the delete fails.**Workaround:** Reload the SSM.
- CSCsk95241  
**Symptom:** If you use JDK instead of JRE on Solaris, you might encounter a problem trying to install Device Manager from a web browser. This can happen because the installer heap limit of 256 MB is not sufficient.  
**Workaround:** If you have this problem, save the **jnlp** link as file, increase the heap limit to 512 MB, and run **javaws element-manager.jnlp** at the shell prompt.



**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- CSCs112130

**Symptom:** After a disruptive downgrade or upgrade between SAN-OS Release 3.2(2c) and Release 3.2(1a), issuing a no shutdown command on a Cisco SME interface fails. When issuing the install all command to perform the downgrade process, a warning is issued that indicates that the downgrade will be disruptive if Cisco SME is enabled.

**Workaround:** Disable Cisco SME before proceeding with the downgrade process. If you perform a disruptive downgrade, then issue the **purge module slot running-config** command for the MSM-18/4 modules where Cisco SME is configured after the downgrade is complete.
- CSCs115511

**Symptom:** On the MDS 12-port, 24-port, and 48-port 4-Gbps Fibre Channel switching modules, and on the 4-port 10-Gbps Fibre Channel switching module for downgrades from 3.2(2c) to lower versions, if fcdomain persistency is disabled, F ports may not come up after a **shutdown** or **no shutdown** or a link flap.

**Workaround:** Shut the F port, enable and disable fcdomain persistency for that VSAN, and then bring up the F port.
- CSCs117944

**Symptom:** During an MDS 9222i switch reload, the connection from the management port (mgmt0) to the Gigabit Ethernet interface goes down. When the connection comes back up, the Gigabit Ethernet interface doesn't go into forwarding mode until 30 seconds later. The Fabric Manager server is not able to communicate to the MDS 9222i switch through SNMP during this 30 second window.

**Workaround:** If the switch is in the Cisco Ethernet switch family, configure port-fast to resolve the issue. On Ethernet switches from other vendors, apply a similar configuration mode.
- CSCs131087

**Symptom:** In DMM, if a server I/O to a LUN fails during data migration, that session is marked as failed. The DMM migration job is then moved to a Failed state when the remaining sessions are complete. Such a failed migration job can be scheduled for a restart. If such a failed migration job is scheduled to start in less than 5 minutes from the time of scheduling, and another server I/O to a session LUN fails in that 5 minute window, the migration job will move from a Scheduled state to a Failed state. An administrator has the option to start the job immediately or schedule it again. This problem does not happen if an administrator schedules the migration job to start more than 5 minutes from the time of scheduling.

**Workaround:** Schedule the data migration job to start more than 5 minutes from the time of scheduling.
- CSCs133763

**Symptom:** In Cisco SME, tape device names can not include special characters (such as hyphens or underscores). This will cause future tape device creations for a tape group to fail.

**Workaround:**
- CSCs134922

**Symptom:** Dual-fabric DMM migration jobs can not have one fabric running Release 3.2(1a) and a peer fabric running Release 3.2(2c) due to a signal message change. This may cause unexpected results during a DMM migration job validation, creation, start, and so on.

**Workaround:** Run both fabrics with the same software image.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- CSCs165951

**Symptom:** Using Fabric Manager Release 3.2(2), an error is displayed in the creation wizard. This occurs when an enclosure spans multiple fabrics and not all fabrics are managed and when the Data Migration Wizard is used to create a job with that enclosure as the existing storage (selecting all ports listed in that enclosure).

**Workaround:** Put the ports you plan to use as the existing storage in the migration into a separate enclosure, and use that enclosure in the wizard selection.
- CSCsi56167

**Symptom:** The response time shown in the output of a **ping ip-address** command may not be accurate if there is an MDS MSM-8/4 in the path.

**Workaround:** Use the **ips measure-rtt** command to measure the round trip time.
- CSCsk91974

**Symptom:** When you issue the **show tech-support sme** or the **show klm internal isapi\_scsi** command after attaching to a module, you may see this error message: `cat: write error: Bad address`. This issue does not affect the actual tech-support log.

**Workaround:** None.
- CSCsk73654

**Symptom:** In certain tape libraries, the tape drives are exported as LUNs. If these target ports are already a part of a Cisco SME configuration and new tape drives are added as LUNs, the new tape drives will not be discovered during a Cisco SME tape group or tape device configuration.

**Workaround:** Perform a rescan at the host level or a flap of the target port to allow Cisco SME to rediscover these newly added tape drives.
- CSCsk43927

**Symptom:** The following Fabric Manager client components that use SSH and Telnet do not work well with NAT:

  - DMM storage job creation
  - Cisco SAN-OS software upgrade
  - Zone activation

**Workaround:** None.
- CSCsk90998

**Symptom:** The signal loss counters in the output of the **show interface fcx/y** command are not incremented.

**Workaround:** None.
- CSCsm13002

**Symptom:** In rare cases, if a READ command issued by Cisco SME for media identification is dropped or lost, the tape is marked as a clear-text tape. Subsequently, a CHECK\_CONDITION with ILI is returned when a READ is issued by the host. This can cause a backup application to mark the tape as read-only.

**Workaround:** Unmount and remount the tape from the backup application to resolve this issue.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- CSCsm15874  
**Symptom:** In rare cases, when Cisco SME attempts to perform a tape device discovery of the backend tapes, a SCSI command can stall. This may cause Cisco SME to remain in the device discovery phase.  
**Workaround:** Reload the module.
- CSCsm17768  
**Symptom:** There is a observable performance drop for backup and restore when Cisco SME is introduced between a host and tape due to the increased latency.  
**Workaround:** None.
- CSCsm18303  
**Symptom:** In certain cases with the Tape Recycle policy enabled in Cisco SME, a new key is generated when a tape is recycled and the old key is not purged.  
**Workaround:** Manually purge the older version of the key.

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents.

### Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

### Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS Storage Services Module Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

### Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

### Hardware Installation

- *Cisco MDS 9124 Multilayer Fabric Switch Quick Start Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*

## Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Database Schema*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*

## Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*

## Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*

## Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*
- *Cisco 10-Gigabit X2 Transceiver Module Installation Note*
- *Cisco MDS 9000 Family CWDM Installation Note*
- *Cisco MDS 9000 Family CWDM Passive Optical System Installation Note*

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***