

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



## Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.2(1a)

**Release Date:** October 6, 2007

**Part Number:** OL-14116-02 M0

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 47.



**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](http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html)

Table 1 shows the on-line change history for this document.

**Table 1** Online History Change

Revision	Date	Description
A0	10/06/2007	Created release notes.
B0	10/18/2007	Added DDTS <a href="#">CSCsj72662</a> .
C0	10/22/2007	Changed the status of DDTS CSCsh31236 to Resolved.
D0	10/23/2007	Added DDTS <a href="#">CSCsk93834</a> . Removed DDTS CSCsh31236. Added a description of a new CLI Command to recover the modflash partition to the “ <a href="#">New Features in Cisco MDS SAN-OS Release 3.2(1a)</a> ” section.
E0	04/23/2008	Added DDTS <a href="#">CSCsk48149</a> .
F0	04/30/2008	Added DDTS <a href="#">CSCso63465</a> .
G0	07/09/2008	Added <a href="#">Upgrading to Recover Loss of Performance Manager Data</a> . Added <a href="#">NPV and NPIV Requirements</a> .



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

© 2008 Cisco Systems, Inc. All rights reserved.

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

**Table 1 Online History Change**

Revision	Date	Description
H0	11/13/2008	Added the “Performing a Nondisruptive Software Upgrade on Generation 1 Modules” section.
I0	11/18/2008	Added DDTS <a href="#">CSCso72230</a> .
J0	01/15/2009	Removed iSNS from the “Changes in Existing Features” section.
K0	04/14/2009	Updated DDTS <a href="#">CSCsk49634</a> .
L0	04/29/2009	Added the “FICON Supported Releases and Upgrade Paths” section. Revised “FICON Downgrade Paths” section. Added the “Compatibility of Fabric Manager and Data Mobility Manager” limitation.
M0	08/28/2009	Removed the DS-SFP-GE-T from <a href="#">Table 1</a> because it is supported on switches running SAN-OS Release 3.3(1) or later.

## Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Components Supported, page 3](#)
- [Software Download Process, page 8](#)
- [Upgrading Your Cisco MDS SAN-OS Software Image, page 11](#)
- [Downgrading Your Cisco MDS SAN-OS Software Image, page 21](#)
- [New Features in Cisco MDS SAN-OS Release 3.2\(1a\), page 24](#)
- [Changes in Existing Features, page 30](#)
- [Limitations and Restrictions, page 30](#)
- [Caveats, page 36](#)
- [Related Documentation, page 47](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 49](#)

## 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.

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

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 2](#) 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 2** Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S2K9-3.2.1A	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.2.1A	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S2K9-3.2.1A	MDS 9222 Supervisor/Fabric-2, SAN-OS software.	MDS 9200 Series only
	M92S1K9-3.2.1A	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S2K9-3.2.1A	MDS 9100 Supervisor/Fabric-2, SAN-OS software.	MDS 9100 Series only
	M91S1K9-3.2.1A	NDS 9100 Supervisor/Fabric-I, SAN-OS software	MDS 9100 Series only

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

**Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)**

Component	Part Number	Description	Applicable Product
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
	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
	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 2 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 <sup>1</sup> sold separately).	MDS 9513 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 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 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 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 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 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 only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 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 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 only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 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

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

**Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)**

Component	Part Number	Description	Applicable Product
	DS-IBM-FC-K9	Cisco Fabric Switch for IBM BladeCenter (includes fourteen internal and six external ports)	Cisco Fabric Switch for IBM BladeCenter only
External crossbar module	DS-13SLT-FAB1	MDS 9513 crossbar fabric module.	MDS 9513 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
	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
	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
	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
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
	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 2 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-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
	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 <sup>2</sup>	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 <sup>3</sup> 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	M90FM-CD-321=	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 8](#)
- [Downloading Software, page 8](#)
- [Selecting the Correct Software Image for an MDS 9200 Series Switch, page 9](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 10](#)
- [Configuring Generation 2 Switching Modules, page 10](#)

## 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](mailto: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](mailto: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 3](#).

**Table 3**      *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 4](#).

**Table 4**      *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-s1ek9

## 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 5](#).

**Table 5**      *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

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

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:

```
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](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](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:

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

[http://www.cisco.com/en/US/products/ps5989/products\\_device\\_support\\_table09186a00805037ee.html](http://www.cisco.com/en/US/products/ps5989/products_device_support_table09186a00805037ee.html)

## 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:

- [Performing a Nondisruptive Software Upgrade on Generation 1 Modules](#), page 11
- [Upgrading Your Version of Cisco Fabric Manager](#), page 12
- [General Upgrading Guidelines](#), page 14
- [Upgrading an MDS 9216 Switch with iSCSI Enabled](#), page 16
- [Upgrading with IVR Enabled](#), page 17
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(1a\)](#), page 18
- [Upgrading the SSI Image on Your SSM](#), page 19
- [Upgrading a Switch with Insufficient Space for Two Images on the Bootflash](#), page 20
- [Upgrading a Cisco MDS 9124 Switch](#), page 20
- [Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch](#), page 21

### Performing a Nondisruptive Software Upgrade on Generation 1 Modules

Generation 1 modules may reload during a nondisruptive SAN-OS software upgrade because of the CompactFlash being unable to partition for the new code. If that happens, the installer aborts and reloads the module.

This issue affects the following modules:

- DS-X9016, 16-port 1-Gbps/2-Gbps Fibre Channel module
- DS-X9032, 32-port 1-Gbps/2-Gbps Fibre Channel module
- DS-X9032-SSM, 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

This issue might be seen during an upgrade from Cisco SAN-OS Release 3.0(x), 3.1(x) or 3.2(x). It has been addressed for upgrades from SAN-OS Release 3.3(1) or higher. Therefore, you will not be impacted by this issue if you are running SAN-OS Release 3.3(1) when you upgrade to a higher SAN-OS release.

When this problem occurs, the module will automatically reload and may cause the Install All to stop, which will cause the upgrade to be unsuccessful. Error messages similar to the following may be displayed:

```
Install has failed. Return code 0x40930020 (Non-disruptive upgrade of a module failed).
Please identify the cause of the failure, and try 'install all' again.
Module 2: Non-disruptive upgrading.
-- FAIL. Return code 0x40690009 (Error in downloading image for image upgrade).
```

To avoid this kind of unplanned disruption, follow the methods for identifying and correcting this issue described in [Cisco Field Notice 63099](#), before proceeding with the SAN-OS upgrade. This Field notice can be found under the [Support, Products page for Cisco MDS9500 Series Multilayer Directors](#) selection.

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

The caveat associated with this issue is CSCsm62295.

## 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. For a complete description of the changes in Fabric Manager, see the “[Cisco Fabric Manager Enhancements](#)” section on page 29.

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)
  - PostgreSQL 8.1 (Solaris and Linux)
  - 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

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

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.
  - Step 3** Copy the Fabric Manager jar file **m9000-fm-3.2.1a.jar** from the CD-ROM to a folder on the Solaris workstation.
  - Step 4** Launch the installer using the following command:
 

```
java -Xmx256m -jar m9000-fm-3.2.1a.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**.

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

- 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(1a).

---

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(1a):

- 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 20](#).
- 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 21](#).
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:
  - **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively upgraded. See [Table 6](#) 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. 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.
  - **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 17](#) for these instructions.

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

- **FICON:** If you have FICON enabled, the upgrade path is different. See [Table 7](#).

Use [Table 6](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.2(1a). 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 6](#) applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

**Table 6 Nondisruptive Upgrade Path to SAN-OS Release 3.2(1a)**

<b>Current</b>	<b>Nondisruptive Upgrade Path</b>
SAN-OS 3.2(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(4)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.1(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.0(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.0(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.0(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.0(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 3.0(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 2.1(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 2.1(2e)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 2.1(2d)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 2.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(1a).
SAN-OS 2.1(2)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(1a).
SAN-OS 2.1(1b)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(1a).

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

**Table 6 Nondisruptive Upgrade Path to SAN-OS Release 3.2(1a) (continued)**

Current	Nondisruptive Upgrade Path
SAN-OS 2.1(1a)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(1a).
SAN-OS 2.0(x)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(1a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(1a).
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(1a).

## FICON Supported Releases and Upgrade Paths

Cisco MDS SAN-OS Release 3.2(1a) does not support FICON.

Table 7 lists the SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

**Table 7 FICON Supported Releases**

FICON Supported Releases	
NX-OS	Release 4.1(1c)
SAN-OS	Release 3.3(1c)
	Release 3.2(2c)
	Release 3.0(3b)
	Release 3.0(3)
	Release 3.0(2)
	Release 2.0(2b)

## Upgrading an MDS 9216 Switch with iSCSI Enabled

Following a software upgrade to Cisco SAN-OS Release 3.2(1a) on a Cisco MDS 9216, 9216A, or 9216i Switch, you need to enable iSCSI on all modules where iSCSI interfaces were present before the upgrade. Use the **iscsi enable module slot-number** command to enable iSCSI, then issue the **copy running-config startup-config** command to have the configuration take effect.

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

## 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); therefore, you must upgrade to Release 2.1(2b) before upgrading to Release 3.2(1a). 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 12](#). 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-fcdomain-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.



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

- Step 3** Check the syslog messages 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.

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

- 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(1a).



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

## Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2(1a)

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(1a).

For more information on upgrading SAN-OS software, see the [“Upgrading Your Cisco MDS SAN-OS Software Image” section on page 11](#).

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
```

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

**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
```

**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\(1a\)](#)” section on page 18.
  - 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

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

## 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

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(1a) on a Cisco MDS 9124 Switch, follow these guidelines:

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

- 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

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path shown in [Table 6](#), 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(2b) to SAN-OS Release 3.2(1a)), 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 21](#)
- [Downgrading the SSI Image on Your SSM, page 24](#)

### General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.2(1a):

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

- 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 8](#) 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. 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 or a MPS-14/2 module is online in the switch. Otherwise, the downgrade will disrupt traffic.
  - **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 17](#) for these instructions.
  - **FICON:** If you have FICON enabled, the downgrade path is different. See [Table 9](#).
  - **iSNS:** The iSNS feature does not support a graceful downgrade from Cisco MDS SAN-OS Release 3.2(1a) to any earlier SAN-OS release. Prior to a downgrade from Cisco SAN-OS 3.2(1a), disable the MDS iSNS server and remove all configurations associated with the MDS iSNS client.

Use [Table 8](#) to determine your nondisruptive downgrade path from Cisco SAN-OS Release 3.2(1a). 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 8](#) applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

**Table 8**      **Nondisruptive Downgrade Path from SAN-OS Release 3.2(1a)**

To SAN-OS Release	Nondisruptive Downgrade Path
SAN-OS 3.2(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.1(4)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.1(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).

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

**Table 8 Nondisruptive Downgrade Path from SAN-OS Release 3.2(1a)**

To SAN-OS Release	Nondisruptive Downgrade Path
SAN-OS 3.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.1(2a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.1(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.1(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.0(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.0(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.0(2a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.0(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 3.0(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 2.1(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 2.1(2e)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 2.1(2d)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
SAN-OS 2.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(1a).
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.

## FICON Downgrade Paths

Cisco MDS SAN-OS Release 3.2(1a) does not support FICON.

Refer to [Table 7](#) for a list SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON downgrade path information.

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

## 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(1a) 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.

## New Features in Cisco MDS SAN-OS Release 3.2(1a)

Cisco MDS SAN-OS Release 3.2(1a) does not include any new features, but it provides all the new features of Cisco MDS SAN-OS Release 3.2(1). This section briefly describes those features. For detailed information about the features listed, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#) and the [Cisco MDS 9000 Family Fabric Manager 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.

### Cisco MDS 9134 Multilayer Fabric Switch

The Cisco MDS 9134 Multilayer Fabric Switch is a 32-port 1-, 2-, and 4-Gbps autosensing Fibre Channel and 2-port 10-Gbps switch. It features On-Demand Port Activation Licensing. By default, the first 24 ports are licensed. An additional license is required for the remaining 8 ports. The 210-Gbps ports are not licensed by default, but require a separate license.

### Cisco MDS 92221 Multiservice Switch

The Cisco MDS 9222i Multiservice Modular Switch offers eighteen 4-Gbps Fibre Channel ports and four Gigabit Ethernet IP storage services ports, and a modular expansion slot to host Cisco MDS 9000 Family Switching and Services Modules.

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

The MDS 9222i switch provides the cryptographic engine used by Cisco Storage Media Encryption. The Cisco MDS 9222i also supports non-disruptive, in services software upgrades (ISSU).

## Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)

The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) offer eighteen 1-, 2-, and 4-Gbps Fibre Channel ports and four Gigabit Ethernet IP storage services ports. Its multiprotocol capabilities integrate in a single-form-factor Fibre Channel, Fibre Channel over IP (FCIP), Small Computer System Interface over IP (iSCSI), IBM Fiber Connectivity (FICON), FICON Control Unit Port (CUP) management, and switch cascading.

The Cisco MDS-18/4 Module can be used with the Cisco MDS 9200 Series of Multilayer Fabric Switches and the Cisco MDS 9500 Series of Multilayer Directors.



**Note**

The MSM-18/4 module supports both the IP Storage (IPS) and Storage Services Interface (SSI) images. As of Cisco SAN-OS 3.2(1a), the MSM-18/4 module does not support any SSI or iSAPI application.

## Cisco MDS 9000 18/4-Port Multiservice Module FIPS (MSFM-18/4)

The Cisco MDS 9000 Family 18/4-Port Multiservice Federal Information Processing Standards (FIPS) Module is a FIPS 140-2 Level 3-compliant version of the Cisco MSM-18/4 Module. It provides added security to meet regulatory and industry requirements. FIPS Level 3 certification requires enhanced physical security, including a hard, opaque potting material to deter unauthorized access and tampering.

## Cisco Data Mobility Manager

Cisco MDS Data Mobility Manager (DMM) for the Cisco MDS 9000 family of switches provides capabilities and features that simplify data migration and minimize service disruptions. Data migration is the process of copying data from an existing storage device to a new storage device.

Data migration is done frequently for storage array upgrades and consolidation or replacement of existing Storage. Cisco MDS 9000 Data Mobility Manger (DMM) offers a new data migration approach using a SAN switch based intelligent fabric application. Cisco DMM runs on the Cisco MDS 9000 Storage Services Module (SSM).

The primary purpose of this feature is moving data from existing storage array to a new storage array. Cisco DMM features include:

- Online migration of heterogeneous arrays
- Simultaneous migration of multiple LUNs
- Unequal size LUN Migration
- Rate adjusted migration
- Verification of migrated data
- Dual fabric support
- CLI and wizard-based management with Cisco Fabric Manager

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

The Cisco DMM can be introduced without having to reconfigure or rewire the existing SAN infrastructure, and migration can be enabled/disabled via software control from the Cisco Fabric Manager. Cisco DMM can be used in SANs which have only Cisco MDS 9000 switches as well as those containing a heterogeneous mixture of Cisco and other vendor switches.

## N-Port Virtualization

The N-Port virtualization (NPV) feature reduces the number of Fibre Channel domain IDs in core-edge SANs. Switches operating in the NPV mode do not join a fabric, they just pass traffic between core switch links and end-devices, which eliminates the domain IDs for these edge switches. This feature is available only for Cisco MDS 9000 blade switches, the Cisco MDS 9124 Multilayer Fabric Switch, and the Cisco MDS 9134 Multilayer Fabric Switch.

The NPV mode applies to an entire switch. All end devices connected to a switch in the NPV mode must log in as N-port to use this feature. Loop attached devices are not supported. All links from the edge switches in NPV mode to the core switches are established as N-ports, not E-ports as used for a typical inter-switch links. Instead, N-Port Identifier Virtualization (NPIV) is used by the switches in NPV mode to log in multiple end-devices that share a link to the core switch.

## NPV and NPIV Requirements

Table 9 shows the minimum SAN-OS release that supports NPV.

**Table 9 NPV SAN-OS Requirements**

Switch	Minimum SAN-OS Release
MDS 9124, MDS 9134	Release 3.2(1)

Table 10 shows the minimum SAN-OS releases that support NPIV.

**Table 10 NPIV Core SAN-OS Requirements**

Switch	Minimum SAN-OS Release
MDS 9124, MDS 9134	Release 3.2(2c)
MDS 9200, MDS 9500	Release 3.2(1)

NPIV is not supported on the MDS 9020 switch and the MDS 9040 switch.



### Note

Upgrades from any of the versions listed in the table above with NPIV enabled will be non-disruptive. If you have not yet enabled NPIV and you are planning to enable NPIV, you should upgrade to one of the versions listed above or later before enabling NPIV.



### Note

When upgrading from Release 3.2(1x) or an earlier release, to Release 3.2(2x) or later on an MDS 9124 or MDS 9134 switch with NPIV enabled, you must disable NPIV before upgrading for a non-disruptive upgrade. This will limit the disruption to ports already logged in using NPIV; other traffic will not be affected. With NPIV turned on, the upgrade will be disruptive.

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

## Digital Diagnostic Enhancements

The digital diagnostics capabilities for small form-factor pluggable (SFP) and 10 Gbps X2 form factor optics have been enhanced in Cisco SAN-OS release 3.2(1a):

- Added support for Dense Wave Division Multiplexing (DWDM) SFPs
- Traps can be generated when digital diagnostic thresholds are exceeded
- Digital diagnostic values are viewable in Cisco Fabric Manager (previously only through CLI)

## Universal Serial Bus Support

The two Universal Serial Bus (USB) 2.0 compatible ports on the Cisco MDS 9500 Series Supervisor-2 modules are available for use with Cisco SAN-OS release 3.2(1a). USB flash drives connected to these ports may be used for the same functions as media in the external compact flash slot.

## Intelligent Fabric Application Enhancements

Several intelligent fabric application enhancements are included in Cisco SAN-OS 3.2(1a):

- SANTap Enhancements include:
  - Dynamic LUNs – support for notifying hosts when LUNs appear/disappear. Currently, SANTap only supports new LUNs being added, but not removed.
  - 32-Bit LUN ID Support – for SSM hardware improves support for newer disk arrays that require greater than 16-bits to identify a LUN.
  - Scalability Enhancements – improves failover performance to allow the number of initiator/target/LUN (ITLs) supported to be increased from 1000 to 2000.
- Software Image Compatibility Check – verifies the compatibility of partner software with the SAN-OS storage services interface (SSI) version before loading it.
- Partner Software Reset – allows network hosted applications to be reset without reloading a SSM.

## FIPS Support

Federal Information Processing Standards (FIPS) 140-2 level 2 qualification has been completed for the Cisco MDS 9000 family. Customers choosing to implement FIPS level 2 security in the SAN select the FIPS mode for switch security.

The FIPS mode has been enhanced to support the Cisco MDS 9000 14/2-Port Multiprotocol Services Module.

## TACACS+ Password Expiry Notification

When an end-user authenticates to a Cisco MDS 9000 switch via a TACACS+ account, this feature lets them know when a password has expired or is about to expire. If the password has expired, the end-user is prompted to change the password.

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

## SMI-S Enhancements

Indications supported has been expanded to allow meaningful monitoring of Cisco MDS 9000 family switches. The following indications have been added:

- Switch FC port status change
- Switch environmental failure
- Zoneset activated
- Switch field replaceable unit change

## Common Criteria

Validation of Common Criteria (CC) evaluation assurance level 3 (EAL 3) for the Cisco MDS 9000 Family members running Cisco SAN-OS 3.0(2a) shall be achieved by the release 3.2(1a) time frame.

Common Criteria is an international standard (ISO/IEC 15408) for computer security that provides assurance that the process of specifying, developing, and evaluating security features have been conducted in a rigorous manner, enabling evaluators to determine if a product meets its security requirements.

## Server LUN Map Discovery Commands

Server LUN map discovery commands have been added to the CLI to discover all LUNs in a disk array that are masked for access by a particular host. You can specify a VSAN, a specific host interface, and the targets to query. The commands allow you to find LUNs that are zoned, and also LUNs that are not zoned if the disk array allows this. A Cisco MDS 9000 Storage Services Module (SSM) is required to use this feature.

## New MIBS

The following new MIB is included in Cisco MDS 9000 SAN-OS release 3.2(1a):

- CISCO-DMM-MIB

## In-service Software Upgrades for the Cisco MDS 9222i Switch

Cisco SAN-OS 3.2(1a) includes non-disruptive, in service software upgrades (ISSU) for the Cisco MDS 9222i switch. This feature does not apply to the Cisco MDS 9216 and 9216i fabric switches.

## New CLI Command to Recover the Modflash Partition

The infrastructure of the Storage Services Module (SSM) includes a non-volatile modflash partition to store partner specific images and configuration files. Any detectable partitioning and file system errors are automatically repaired during the module initialization procedures. However, certain types of file system errors cannot be auto-detected or auto-repaired. Manual procedures might be required to recover from these types of errors. This recovery procedure is destructive, since it reformats and recreates the modflash partition. All data in the modflash partition is deleted. SSM initial provisioning procedures

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

need to be followed for completing the recovery procedure. For these situations, a new CLI command is included in Cisco MDS SAN-OS Release 3.2(1a). The following example shows the **debug mkfs modflash** command.

```
switch# attach module slot
Attaching to module x ...
To exit type 'exit', to abort type '$.'
module-slot# debug mkfs modflash
```

## Cisco Fabric Manager Enhancements

### New Installation Process

Starting in release 3.2(1a), the installation process for Cisco Fabric Manager is changing to accommodate three significant enhancements:

- Cisco Fabric Manager is no longer embedded in the SAN-OS software, which means that Fabric Manager can no longer be installed from a Cisco MDS 9000 Family switch. Only the Device Manager can be installed from a Cisco MDS 9000 Family switch using Java Web Start.
- The relational database that is needed for Fabric Manager is now separate from the Fabric Manager software.
- There are two distinct versions of Cisco Fabric Manager:
  - Fabric Manager Standalone (a single, simplified application)
  - Fabric Manager Server (multiple client, single-server applications)

Cisco Fabric Manager can now be installed from a CD-ROM or from files downloaded from the Cisco web site. To install Fabric Manager Server, you can get the software from the CD-ROM or from a Jar file, and install the PostgreSQL database and the Fabric Manager Server. To install a Fabric Manager Client, you can install the software from the Fabric Manager Server and install the Fabric Manager Client (without a database) and Cisco Device Manager.

The installation process has been broken down into a few large steps for added flexibility. A manual workflow is provided on the CD-ROM to guide the end user through installing a Java Virtual Machine (JVM) if one is not present, installing PostgreSQL database or connecting to an existing Oracle instance, and installing the Cisco Fabric Manager framework and application.

For general guidelines about the Fabric Manager installation process, see [“Upgrading Your Version of Cisco Fabric Manager” section on page 12](#). For complete Fabric Manager installation instructions, refer to the “Installation of Cisco MDS SAN-OS and Fabric Manager” section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, or use the on-screen instructions provided with the CD-ROM.

### Custom Report Enhancements

Several enhancements to the Cisco Fabric Manager custom reports are included in release 3.2(1a). These licensed Cisco FMS features include:

- Additional Report Types
- Report Scheduling
- Topology Maps in FMS Reports
- Fixed Y-Axis Range for Charts

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

## Analysis Reports

Cisco Fabric Manager Server release 3.2(1a) analysis reports present an additional level of information, by compiling results from running specific test programs and more complex analysis of Cisco Fabric Manager Server (FMS) database statistics.

The analysis reports in Cisco FMS release 3.2(1a) are licensed features. They include:

- Connectivity
- Zoning Discrepancies
- Multipathing
- Switch Health
- Fabric Configuration

## Threshold Configuration Flexibility

Cisco Fabric Manager Server allows two performance thresholds to be configured for throughput values for connections to end devices and inter-switch links (ISLs). Prior to Cisco Fabric Manager release 3.2(1a) the user interface forced users to select either a fixed percentage or auto-baseline setting for both. Now end-users can set one threshold for a link based on a fixed percentage and the other using the auto-baseline setting.

# Changes in Existing Features

## iSCSI

As of Cisco SAN-OS Release 3.2(1a), iSCSI should be enabled at the module level.

## SAN Device Virtualization Scalability

Cisco SAN-OS Release 3.2(1a) supports 800 SAN device virtualization (SDV) virtual devices, with 4 secondary real devices mapped to each SDV virtual device in a VSAN.

# Limitations and Restrictions

This section lists the limitations and restrictions for this release.

## Upgrading to Recover Loss of Performance Manager Data



### Caution

You must upgrade to Fabric Manager Release 3.1(x) and then upgrade to a later release of Fabric Manager to avoid losing Performance Manager data. If data has been lost, follow the steps below to recover the data.

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

- 
- Step 1** Disable Performance Manager interpolation using Fabric Manager Web Client. Uncheck **Interpolate missing statistics**, then click **Apply**.
  - Step 2** Stop the Fabric Manager Server.
  - Step 3** Save the data file in the `$INSTALL_DIR` directory.
  - Step 4** Move the old RRD file into the `$INSTALL_DIR/pm/db` directory.
  - Step 5** Run `$INSTALL_DIR/bin/pm.bat m`.
  - Step 6** Restart Fabric Manager Server.
- 

## Java Web Start

When using Java Web Start, it is recommended that you do not use an HTML cache or proxy server. You can use the Java Web Start Preferences panel to view or edit the proxy configuration. To do this, launch the Application Manager, either by clicking the desktop icon (Microsoft Windows), or type `./javaws` in the Java Web Start installation directory (Solaris Operating Environment and Linux), and then select **Edit>Preferences**.

If you fail to change these settings, you may encounter installation issues regarding a version mismatch. If this occurs, you should clear your Java cache and retry.

## Data Mobility Manager

Use the following guidelines when running Cisco Data Mobility Manager:

- If you have a DMM configuration, the DMM job may transition to a Reset state during a supervisor switchover. In that case, the administrator should recover from the Reset state by following the instructions in the *Cisco MDS 9000 Data Mobility Manager Configuration Guide*.
- A storage type job in DMM cannot be restored from a saved ASCII configuration. When a storage job is created in DMM, the SSM generates Virtual Initiators (VIs) for each storage type job. Each request to generate VIs can potentially return different VI pWWNs. As a result, if an ASCII configuration for a storage type job is reapplied, there is a possibility the the VIs generated by the SSM are different. In that case, the session configurations in the saved configuration are no longer valid.
- Following a **fcdomain restart disruptive** command, the DMM process cleans up all configurations and transitions the DMM job in the affected VSAN to the Reset state. During the cleanup, some virtual devices are not deleted correctly, which results in an incomplete cleanup. As a result, when the administrator validates the DMM job from the CLI or restarts or schedules the DMM job from Fabric Manager, the operation fails. If this situation occurs with a DMM job configured on the SSM, then reload the SSM to recover the DMM job.
- For active-passive arrays, DMM requires that the administrator create two DMM jobs: one for the active LUNs from one controller and the other for the active LUNs on the other controller. DMM provides the Server Lunmap Discovery (SLD) tool to detect if the array is in fact active-passive. On

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

the IBM DS-4500 storage device, the SLD cannot successfully detect active-passive LUNs on a storage port. As a consequence, the administrator will have to determine which LUNs are active on which port and create DMM jobs accordingly.

- A DMM job that is in progress might fail if you change the clock on an MDS switch by configuring the NTP server.

## Compatibility of Fabric Manager and Data Mobility Manager

Cisco Fabric Manager in any MDS NX-OS 4.1(x) release does not support Data Mobility Manager (DMM) in any SAN-OS 3.3(x) release or in any 3.2(x) release. To use the Cisco Fabric Manager GUI for DMM, both Fabric Manager and DMM must be running NX-OS or SAN-OS software from the same release series.

## Cisco MDS 9134 Multilayer Fabric Switch

The Cisco MDS 9134 Multilayer Fabric Switch does not support the following Cisco MDS SAN-OS features:

- IVR
- Remote Span
- Translative loop support
- FCC - no generation, quench reaction only

In addition, the following features have these limits:

- VSANs - 16 maximum
- SPAN - 1 session maximum

## Using NPIV on Cisco Fabric Switches

In Cisco SAN-OS Release 3.2(1a), the Cisco MDS 9134 Switch, the Cisco MDS 9124 Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter do not support hardware-enforced zoning for devices attached to an F port that is participating in NPIV. This capability will be supported in a future release.

If NPIV is enabled on a Cisco MDS 9134 Switch, the Cisco MDS 9124 Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter and one of the devices connected through an F port that is participating in NPIV goes down, all devices connected through the same F port will lose connectivity. This situation can be corrected by issuing the **shutdown** command, followed by the **no shutdown** command. This issue will be resolved in a future release.

## Cisco MDS 9222i Multiservice Modular Switch and Cisco MDS 9000 18/4-Port Multiservice Module

The Cisco MDS 9222i Multiservice Modular Switch and the Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) support one iSCSI forwarding mode that is equivalent to store-forward on the MPS-14/2 module.

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

The Cisco MDS 9222i and the MSM-18/4 support header-digest, but not data-digest in Cisco SAN-OS 3.2(1a).

The Cisco MDS 9222i and the MSM-18/4 do not support Ether channel.

The Cisco MDS 9222i supports only the following modules in slot 2:

- The Storage Services Module (SSM)
- The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)
- The 8-port Gigabit Ethernet IP Storage services module
- The MDS 9000 12-, 24-, and 48-port 4-Gbps Fibre Channel modules
- The MDS 9000 4-port 10-Gbps Fibre Channel module

The MSM-18/4 and MDS 9222i Switch do not support the following features:

- Special frames for FCIP
- B ports for San Extension
- SAN extension tuner
- NetSim
- IPv6
- FCIP between the MSM-18/4 and another IPS module

## Using SAN Device Virtualization on Cisco Fabric Switches

There must be at least one SAN device virtualization-enabled switch that is not a Cisco MDS 9124 switch, a Cisco Fabric Switch for HP c-Class BladeSystem, or a Cisco Fabric Switch for IBM BladeCenter between the server and the target that are being virtualized. In other words, SAN device virtualization does not work when initiators and primary targets are connected to the same Cisco MDS 9124 Switch or or Cisco MDS 9134 Switch or Cisco Fabric Switch for HP c-Class BladeSystem or Cisco Fabric Switch for IBM BladeCenter.

## CWDM SFPs

The 2-Gbps CWDM SFPs do not have have a maximum speed set in memory and they negotiate to 4-Gbps on modules that support the higher speed. As a result, the link comes up and appears to work, but then becomes disabled and connectivity problems occur. To correct this problem, both sides of the connection must have their speed hard coded to 2-Gbps.

## Fabric Manager

Observe the following limitations or restrictions for the Cisco SAN-OS Release 3.2(1a) for Fabric Manager:

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

- By default, the database and aaa passwords are stored in plain text. You can encrypt them by using the `encrypter.bat/.sh` script and pasting the output into the appropriate file, either `server.properties` or `aaa.properties`.
- The Microsoft Security Patch MS06-040 is known to break applications with a large heap memory. If you increase any Java application's heap (including Fabric Manager) beyond 64 M, we recommend you do not apply this patch.
- If port 80 on the switch is blocked and you are using VPN, Fabric Manager cannot detect NAT addresses. The timeout for URL connections is set for 500ms.

## **MTU Size Limitation**

The Cisco MDS 9216i switch and MPS-14/2 module do not support an MTU size greater than 8000 bytes. An attempt to set the MTU size greater than 8000 bytes will result in an error. As a workaround, reset the value of the MTU size (576 to 8000 bytes) and issue the `no shutdown` command on the interface for normal operation.

## **Reconfiguring SSM Ports**

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 3.1(1). For instructions about how to modify the configuration of the ports before upgrading to SAN-OS Release 3.1(3a), see the [“Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(1a\)”](#) section on page 18.

## **Virtual Router Redundancy Protocol (VRRP) Interfaces**

When a switchover occurs on a switch that is the master for Virtual Router Redundancy Protocol (VRRP) interfaces, the switchover may cause a minor delay. As a result, the VRRP backup (occurring elsewhere) may assume the role of the VRRP master. As a workaround, increase the VRRP advertisement interval for these interfaces.

## **QoS on an MDS 48-port Fibre Channel Module**

Due to possible differences in parts per million between the MAC ASICs on both sides of an ISL link, there is a potential throughput issue when running QoS over an ISL on an MDS 48-port Fibre Channel module. Specifically, the user may not see traffic throughput that follows the programmed QoS ratios. The throughput ratio on the high and/or medium priority class of service (COS) relative to the low priority COS, may not be as high as the actual programmed ratio.

If this situation occurs, you can move the ISL to a port on a different port group on one and/or both sides of the link, or move the ISL to a port on a lower-density card if you require accurate QoS ratios.

## **Maximum Number of Zones Supported in Interop Mode 4**

In interop mode 4, the maximum number of zones that is supported in an active zone set is 2047, due to limitations in the connected vendor switch.

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

When IVR is used in interop mode 4, the maximum number of zones supported, including IVR zones, in the active zone set is 2047.

## Configuring Default Settings for the Default Zone

Following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release, the configuration defined by the **zone default-zone permit vsan vsan-id** command is applied only to the active VSAN. The configuration does not apply to unconfigured VSANs. In SAN-OS 3.x, you can apply the configuration to unconfigured VSANs by issuing the **system default zone default-zone permit** command.

Similarly, the **zoneset distribute full vsan vsan-id** command applies only to the active VSAN following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release.

Although you can configure the default-zone settings in the setup script, these settings do not take effect for VSAN 1, because VSAN 1 already exists prior to running the setup script. To configure the default settings for the default-zone in VSAN 1, you must explicitly enter the **zone default-zone permit** command.

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

# Caveats

This section lists the open and resolved caveats for this release. Use [Table 11](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

**Table 11** Open Caveats and Resolved Caveats Reference

DDTS Number	Software Release (Open or Resolved)	
	3.1(4)	3.2(1a)
<b>Severity 1</b>		
<a href="#">CSCsk56347</a>	O	R
<b>Severity 2</b>		
<a href="#">CSCsg49151</a>	O	O
<a href="#">CSCsi03043</a>	O	R
<a href="#">CSCsi49231</a>	O	R
<a href="#">CSCsi72048</a>	O	O
<a href="#">CSCsi78480</a>	O	R
<a href="#">CSCsj64048</a>	O	R
<a href="#">CSCsj65565</a>	O	R
<a href="#">CSCsj72662</a>	O	R
<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="#">CSCso72230</a>	O	O
<b>Severity 3</b>		
<a href="#">CSCin95789</a>	O	O
<a href="#">CSCsd21187</a>	O	O
<a href="#">CSCse31881</a>	O	O
<a href="#">CSCse47687</a>	O	O
<a href="#">CSCsg19148</a>	O	O
<a href="#">CSCsg19303</a>	O	O
<a href="#">CSCsg62704</a>	O	R
<a href="#">CSCsh05721</a>	O	R
<a href="#">CSCsh63658</a>	O	R
<a href="#">CSCsh70152</a>	O	R
<a href="#">CSCsi07649</a>	O	R
<a href="#">CSCsi51436</a>	O	R
<a href="#">CSCsi56949</a>	O	R

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

**Table 11** Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	3.1(4)	3.2(1a)
<a href="#">CSCsi66310</a>	O	O
<a href="#">CSCsj13175</a>	O	R
<a href="#">CSCsj24904</a>	O	O
<a href="#">CSCsj29134</a>	O	R
<a href="#">CSCsj52389</a>	O	R
<a href="#">CSCsj95379</a>	O	R
<a href="#">CSCsk00953</a>	O	O
<a href="#">CSCsk18352</a>	O	O
<a href="#">CSCsk26424</a>	O	O
<a href="#">CSCsk35725</a>	O	O
<a href="#">CSCsk35951</a>	O	O
<a href="#">CSCsk39341</a>	O	O
<a href="#">CSCsk48149</a>	O	R
<a href="#">CSCsk49309</a>	O	O
<a href="#">CSCsk63929</a>	O	O
<a href="#">CSCsk73520</a>	O	R
<a href="#">CSCsk93834</a>	–	O
<a href="#">CSCso63465</a>	O	O
<b>Severity 4</b>		
<a href="#">CSCsh63896</a>	O	R
<a href="#">CSCsh68830</a>	O	R
<a href="#">CSCsi56167</a>	O	O
<b>Severity 6</b>		
<a href="#">CSCeh35635</a>	O	R
<a href="#">CSCsj74881</a>	–	R
<a href="#">CSCsk43927</a>	O	O
<a href="#">CSCsk68110</a>	O	R

## Resolved Caveats

- [CSCsk56347](#)

**Symptom:** During an in-service software upgrade (ISSU) to Cisco MDS SAN-OS Release 3.2(1a) on a module in an MDS 9500 series switch, the access control list (ACL) process on the module might fail. As a result, the ISSU operation fails, which causes a disruptive reload of the module.

**Workaround:** This issue is resolved.

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

- CSCsi03043
 

**Symptom:** The CIM Server process goes into an unresponsive state after approximately two hours of scheduled probes that associate Fibre Channel ports to each switch.

**Workaround:** This issue is resolved.
- CSCsi49231
 

**Symptom:** 100% CPU utilization was seen on an MDS switch. It was caused by repeated fabric logins (FLOGIs) on a particular port. This situation can occur if a host cannot log in because the allocation of the FC ID fails, and keeps re-trying using a specific pattern of Source FC IDs (S\_IDs) for the FLOGI frame.

**Workaround:** This issue has been resolved. The interface will now be error-disabled for too many FLOGI failures.

To troubleshoot the configuration and find the reason for the FC ID allocation failure, examine the messages in the syslog. Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for detailed information about FLOGI, FC IDs, and FC ID allocation for HBAs.
- CSCsi78480
 

**Symptom:** Under some circumstances, disabling the CIM Server does not terminate the CIM Server process, which causes further enabling or disabling of the CIM Server to be ineffective.

**Workaround:** This issue is resolved.
- CSCsj64048
 

**Symptom:** In rare situations, data virtual target (DVT) configurations might disappear following a reload of the SSM or an upgrade to the SSI 3.1(2m) image.

**Workaround:** This issue is resolved.
- CSCsj65565
 

**Symptom:** Spectra Logic tape drives require a unique area ID.

**Workaround:** This issue is resolved.
- CSCsj72662
 

**Symptom:** Following an upgrade to any Cisco SAN-OS 3.0 release or to any Cisco SAN-OS 3.1 release up to 3.1(4), one or more 4-port blocks on the MDS 9000 16-port Fibre Channel switching module might become disabled. Similarly, one or more 8-port blocks might become disabled on the MDS 9000 32-port Fibre Channel switching module.

You might see output similar to the following from a **show logging log** command:

```
%IMAGE_DNLD-SLOT4-2-IMG_DNLD_STARTED: Module image download process. Please wait
until completion...
%IMAGE_DNLD-SLOT4-2-IMG_DNLD_COMPLETE: Module image download process. Download
successful.
%MODULE-2-MOD_DIAG_FAIL: Module 4 (serial: XYZ) reported failure on ports 4/13-4/16
(Fibre Channel) due to Q-Engine instance shutdown in device 7 (device error
0xc0703572)
%MODULE-2-MOD_SOMEPORTS_FAILED: Module 4 (serial: XYZ) reported failure on ports
4/13-4/16 (Fibre Channel) due to Q-Engine instance shutdown in device 7 (error
0xc0703572)
%PORT-5-IF_DOWN_HW_FAILURE: %$VSAN 4094%$ Interface fc4/16 is down (Hardware Failure)
%PORT-5-IF_DOWN_HW_FAILURE: %$VSAN 4094%$ Interface fc4/15 is down (Hardware Failure)
%PORT-5-IF_DOWN_HW_FAILURE: %$VSAN 1003%$ Interface fc4/14 is down (Hardware Failure)
```

You might see output similar to the following from a **show module internal exceptionlog** command:

```
===== EXCEPTION LOG =====
```

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

```

*** Log# 0 ***
Device Id : 7
Device Name : aladdin
Device Error Code : c0703572(H)
Sys Error : Q-Engine instance shutdown
Errtype : NON-CATASTROPHIC
PhyPortLayer : Fibre Channel
Port(s) Affected : 13-16
Error Description : aladdin instance #3 shutdown: 0xc0703572 DSAP : 0 UUID : 0 Time
: Mon Jul 9 22:33:18 2007
(954381 usecs 823(H) jiffies)

```

**Workaround:** This issue is resolved.

- CSCsg62704

**Symptom:** On an MDS switch with dual supervisor modules, the bootflash on the standby supervisor is replaced with a new bootflash. Then there is a system switchover. Then the bootflash on the new standby supervisor (which was previously the active supervisor) is replaced. The **copy running-config startup-config** command is used to save the configuration, but the console speed does not get saved. Instead, the console speed is reset to 9600.

**Workaround:** This issue is resolved.

- CSCsh05721

**Symptom:** An association call from a VSAN to its logical switch returns a particular WWN, but an association call from the physical system to the virtual system does not return the same WWN, which indicates that the logical switch is not associated to the physical switch.

**Workaround:** This issue is resolved.

- CSCsh63658

**Symptom:** Under rare circumstances, a customer running the Cisco MDS SAN-OS SANTap feature with EMC RecoverPoint might find that following a reload of the SSM module, the SSM CVT is stuck in UNKNOWN status in the RecoverPoint appliance.

**Workaround:** This issue is resolved.

- CSCsh70152

**Symptom:** Memory leaks in the CIM Server could eventually result in the process terminating or becoming unresponsive.

**Workaround:** This issue is resolved.

All known resource leaks in the CIM Server have been fixed. However, some growth in the process size can still be observed when repeatedly executing queries that retrieve large amounts of data.

- CSCsi07649

**Symptom:** When using the Fcanalyzer on an MDS 9513 Switch or an MDS 9124 Switch to capture packets remotely, no packets were captured.

**Workaround:** This issue is resolved.

- CSCsi51436

**Symptom:** Following a fabric reconfiguration, if you use Fabric Manager Server to discover the fabric and you check the **Accelerate Discovery** check box on the Discover New Fabric dialog box, some VSANs are segmented by Fabric Manager Server. VSANs may be segmented because they are isolated or down.

**Workaround:** This issue is resolved.

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

- CSCsi56949  
**Symptom:** When creating a new VSAN through Fabric Manager or through a script that can create a VSAN on each switch at the same time, the same domain ID is created for each switch. This causes the newly-created VSAN to be segmented on all links.  
**Workaround:** This issue is resolved.
- CSCsj13175  
**Symptom:** A fibre channel port on an MDS switching module remained out-of-service after the port was put back in service. As a result, it was not possible to configure the port.  
**Workaround:** This issue is resolved.
- CSCsj29134  
**Symptom:** Following a Cisco SAN-OS software upgrade or downgrade, certain ports get stuck in link failure or in a not-connected state, even though the same SFP, cable, host, or storage device works in other ports on the same module.  
**Workaround:** This issue is resolved.
- CSCsj52389  
**Symptom:** When an fcalias is added as a zone member or a zone is added to a zone set via SNMP, there is an SNMPD memory leak.  
**Workaround:** This issue is resolved.
- CSCsj95379  
**Symptom:** A data path processor (DPP) might fail on an MDS switch running Cisco SAN-OS Release 3.1(2b) with an SSM running SSI Release 3.1(2m) and with the SANTap feature provisioned. The failure occurs while the DPP is processing an unexpected transfer ready message.  
**Workaround:** This issue is resolved.
- CSCsk48149  
**Symptom:** IVR zone set activation in Interop mode 4 results in a failure without an appropriate status message. This issue is seen if a successful IVR zone set activation results in more than 2047 zones in Interop mode 4. In Interop mode 4, the combined number of regular and IVR zones supported is 2047. If an IVR activation attempts to activate more than 2047 zones, the activation is rejected by the zone server module. An appropriate status message is not conveyed back to IVR.  
**Workaround:** This issue is resolved.
- CSCsk73520  
**Symptom:** In some cases, when Fabric Manager Server is installed on hosts with multiple network interfaces, the trap destination IP interface might be incorrectly registered, which results in traps not reaching the Fabric Manager Server.  
**Workaround:** This issue is resolved.
- CSCsh63896  
**Symptom:** After switching over from the active to the standby supervisor, an EMC call home message displays that says the mgmt0 interface has failed on slot 1.  
**Workaround:** This issue is resolved.

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

- CSCsh68830  
**Symptom:** The Java Help search engine in Cisco Fabric Manager and Device Manager does not work correctly in Cisco SAN-OS 3.1(2).  
**Workaround:** This issue is resolved.
- CSCeh35635  
**Symptom:** For passwords authenticated by an AAA server, the MDS switch should inform the user when their password is about to expire.  
**Workaround:** This is an enhancement. It is available only for CLI logins. Fabric Manager and Device currently do not support this feature.
- CSCsj74881  
**Symptom:** If the port license count on an MDS switch is greater than the one supported by the installed platform, ports do not automatically acquire a license. The license must be acquired manually.  
**Workaround:** This issue is resolved.
- CSCsk68110  
**Symptom:** A URL for EMC is needed so that Fabric Manager can be downloaded from EMC.  
**Workaround:** This issue is resolved.

## 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.

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

- CSCsk43922

**Symptom:** A data path processor (DPP) might fail on an MDS switch running SSI Release 3.2(1a) 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.

- 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 (above 100ms RTT and 0.5% loss).

**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 pwwn pwwn 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.

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

- CSCsk51193

**Symptom:** Following an upgrade to Cisco MDS SAN-OS Release 3.2(1a) 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.

- CSCso72230

**Symptom:** In rare instances, the following Generation 2 modules might reload:

- 12-port 4-Gbps Fibre Channel module
- 24-port 4-Gbps Fibre Channel module
- 48-port 4-Gbps Fibre Channel module
- 4-port 10-Gbps Fibre Channel module

The output of the **show logging log** command will have events like those shown below. In the following output, module 7 is the supervisor and module 12 is the module that reloaded.

```
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 7 (serial: JAE1134UR88)
reported warnings on ports 7/1-7/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 8 (serial: JAE1134UOTD)
reported warnings on ports 8/1-8/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:35 fcd95c41 %XBAR-5-XBAR_STATUS_REPORT: Module 12 reported status
for component 88 code 0x40240015.
2008 Jul 15 19:39:35 fcd95c41 %MODULE-2-MOD_DIAG_FAIL: Module 12 (serial: JAE1136VU6L)
reported failure on ports 12/1-12/24 (Fibre Channel) due to Fatal runtime Arb error.
(DevErr is bitmap of failed modules) in device 88 (device error 0x800)
"show logging onboard" will show log similar to the one below for the reloaded module:
Logging time: Tue Jul 15 19:39:28 2008
machine check: process swapper (0), jiffies 0x744af3a4
Free pages in zone[0]:0x4a70,zone[1]:0x0,zone[2]:0x0
Stack: c000dd58 c001eefc c000b2c4 c000ae98 d2060e10 c003d7a4 c00f869c c0045cdc
d196c584 d196d100 c000c31c c000c3e4 c000ae90 c000c910 c000c924 c0008948 c01ca610
c0000394
.....
.....
```

**Workaround:** None. The chance of a module reload occurring again on the same module is very rare. Therefore, continued use of the module is acceptable.

A software workaround for this issue exists in SAN-OS Release 3.3.(2) and NX-OS Release 4.(1b). Upgrading to one of those releases will help decrease instances of modules reloads.

- 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.

- CSCsd21187

**Symptom:** If an iSNS client tries to register a portal separately after registering the network entity and storage node object with the Cisco MDS iSNS server, the portal registration might fail.

**Workaround:** Register the portal at the same time as the network entity and storage node object registration.

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

- 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.
- 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(1a).

**Workaround:** None.
- CSCsj24904
 

**Symptom:** On a Gigabit Ethernet interface on the MDS MSM-18/4, 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.
- 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.

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

- CSCsk18352
 

**Symptom:** If a supervisor switchover occurs while Fabric Manager is creating a DMM job, the job creation process times out.

**Workaround:** Cancel the DMM job and then recreate it.
- CSCsk26424
 

**Symptom:** Removing a fabric and then adding the same fabric in Fabric Manager causes a session fabric ID mismatch. As a result, hosts do not appear in the Step 1 window of the Fabric Manager DMM job creation wizard.

**Workaround:** Restart the Fabric Manager Server.
- 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.
- CSCsk39341
 

**Symptom:** Although the FCIP compression ratio is set to Auto, it does not display correctly in Fabric Manager Server.

**Workaround:** None.
- 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(1a) 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
```
- 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.

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

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.

- CSCso63465

**Symptom:** FCP-CMD (for example, Inquiry) frames targeted to LUN 0x45F0 or LUN 0x50F0 are dropped by an MDS switch when traffic flows (egresses) thru Generation 2 modules. LUN 0x45F0 corresponds to HPUX's Volume Set Address <VBUS ID: 0xB, Target ID: 0xE, LUN: 0x0>.

**Workaround:** Do not use LUN 0x45F0 and LUN 0x50F0 when Generation 2 modules are present in the fabric.

- 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.

- 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.

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

## 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*
- *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*

### Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

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

- *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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0908R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.

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