

Send documentation comments to mdsfeedback-doc@cisco.com.



Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.1(3a)

Release Date: June 24, 2007

Text Part Number: OL-12208-06 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 38.



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

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

Table 1 Online History Change

| Revision | Date | Description |
|----------|------------|---|
| A0 | 06/24/2007 | Created release notes. |
| B0 | 07/18/2007 | Deleted CSCei82909. |
| C0 | 08/29/2007 | Added the 4-Gbps CWDM components to Table 2 . Added a missing SAN-OS Release number to Table 5 and Table 7 . |
| D0 | 09/24/2007 | Added DDTS CSCsi72048 , CSCsi77398 , CSCsj14140 , CSCsj44453 , CSCsj49207 , CSCsj50299 , and CSCsk21652 . |
| E0 | 09/27/2007 | Added DDTS CSCeh35635 , CSCsg49151 , CSCsg62704 , CSCsh05721 , CSCsh63658 , CSCsh70152 , CSCsi49231 , CSCsi56949 , CSCsi78480 , CSCsj13175 , CSCsj29134 , CSCsj52389 , CSCsj64048 , CSCsj65565 , and CSCsj95379 . |
| F0 | 04/23/2008 | Added CSCsk48149 . |
| G0 | 10/17/2007 | Added DDTS CSCsj72662 . |



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 | 10/24/2007 | Removed DDTS CSCsh31236. Added a Note about Downgrading from Cisco SAN-OS 3.2(1) to the “Downgrading Your Cisco MDS SAN-OS Software Image” section. |
| I0 | 04/23/2008 | Added DDTS CSCsk48149. |
| J0 | 04/30/2008 | Added DDTS CSCso63465. |
| K0 | 10/31/2008 | Updated the Symptom description for CSCsj50299. |
| L0 | 11/13/2008 | Added the “Performing a Nondisruptive Software Upgrade on Generation 1 Modules” section. |
| M0 | 11/18/2008 | Added DDTS CSCso72230. |

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Components Supported, page 3](#)
- [Software Download Process, page 6](#)
- [Upgrading Your Cisco MDS SAN-OS Software Image, page 10](#)
- [Downgrading Your Cisco MDS SAN-OS Software Image, page 18](#)
- [New Features in Cisco MDS SAN-OS Release 3.1\(3a\), page 22](#)
- [Limitations and Restrictions, page 25](#)
- [Caveats, page 29](#)
- [Related Documentation, page 38](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 40](#)

Introduction

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

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

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

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 | M95S2K9-3.1.3a | MDS 9500 Supervisor/Fabric-2, SAN-OS software. | MDS 9500 Series only |
| | M95S1K9-3.1.3a | MDS 9500 Supervisor/Fabric-I, SAN-OS software. | MDS 9500 Series only |
| | M92S1K9-3.1.3a | MDS 9216 Supervisor/Fabric-I, SAN-OS software. | MDS 9200 Series only |
| | M91S2K9-3.1.3a | MDS 9100 Supervisor/Fabric-2, SAN-OS software. | MDS 9100 Series only |
| | M91S1K9-3.1.3a | NDS 9100 Supervisor/Fabric-I, SAN-OS software | MDS 9100 Series only |
| | License | M9500ENT1K9 | Enterprise package. |
| 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 |
| 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 |
| M9500SSE1K9 | | Storage Services Enabler package. | MDS 9500 Series with SSM |
| M9200SSE1K9 | | Storage Services Enabler package. | MDS 9200 Series with SSM |
| M9124PL8-4G | | On-Demand Ports Activation License | MDS 9124 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 ¹ 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-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-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 |
| | 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. | |

[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 |
|-------------------------|-----------------|---|--|
| 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. | |
| 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). | |
| LC-type fiber-optic SFP | DS-SFP-FC-2G-SW | 2-Gbps/1-Gbps Fibre Channel—short wavelength SFP. | MDS 9000 Family |
| | DS-SFP-FC-2G-LW | 2-Gbps/1-Gbps Fibre Channel—long wavelength SFP. | |
| | DS-SFP-FCGE-SW | 1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP. | |
| | DS-SFP-FCGE-LW | 1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—long wavelength SFP. | |
| | DS-SFP-GE-T | 1-Gbps Ethernet SFP. | MDS 9500 Series and 9200 Series, except for the MDS 9216 |
| | DS-SFP-FC4G-SW | 4-Gbps/2-Gbps/1-Gbps Fibre Channel—short wavelength SFP for DS-X91xx switching modules. | |
| | 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. | |

Send documentation comments to mdsfeedback-doc@cisco.com.

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

| Component | Part Number | Description | Applicable Product |
|-----------------------|------------------|--|----------------------|
| CWDM ² | DS-CWDM-xxxx | Gigabit Ethernet and 1-Gbps/2-Gbps/4-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm. | MDS 9000 Family |
| | DS-CWDM-MUX-4 | Add/drop multiplexer for four CWDM wavelengths. | |
| | DS-CWDM-MUX-8 | Add/drop multiplexer for eight CWDM wavelengths. | |
| | DS-CWDMCHASSIS | Two slot chassis for CWDM add/drop multiplexers. | |
| Power supplies | DS-CAC-6000W | 6000-W AC power supply. | MDS 9513 only |
| | DS-CAC-2500W | 2500-W AC power supply. | MDS 9509 only |
| | DS-CDC-2500W | 2500-W DC power supply. | |
| | DS-CAC-3000W | 3000-W AC power supply. | |
| | DS-CAC-4000W-US | 4000-W AC power supply for US (cable attached). | |
| | DS-CAC-4000W-INT | 4000-W AC power supply international (cable attached). | |
| | DS-CAC-1900W | 1900-W AC power supply. | MDS 9506 only |
| | DS-CDC-1900W | 1900-W DC power supply. | |
| | DS-CAC-845W | 845-W AC power supply. | MDS 9200 Series only |
| | DS-CAC-300W | 300-W ³ AC power supply. | MDS 9100 Series only |
| CompactFlash | MEM-MDS-FLD512M | 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-212= | 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

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:

Send documentation comments to mdsfeedback-doc@cisco.com.

- [Determining the Software Version, page 7](#)
- [Downloading Software, page 7](#)
- [Selecting the Correct Software Image for an MDS 9500 Series Switch, page 8](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 9](#)
- [Configuring Generation 2 Switching Modules, page 9](#)

Determining the Software Version

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

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



Note

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

Downloading Software

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

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

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

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

Compatibility check is done:

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

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



Note

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

Send documentation comments to mdsfeedback-doc@cisco.com.

**Note**

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

Selecting the Correct Software Image for an MDS 9100 Series Switch

The system and kickstart image that you use for an MDS 9100 series switch depends on which switch you use, as shown in [Table 3](#).

Table 3 Software Image for MDS 9100 Series Switch

| Switch | Image |
|--|----------------------------------|
| MDS 9120 or MDS 9140 | Filename begins with m9100-s1ek9 |
| 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 9500 Series Switch

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

Table 4 Software Image for Supervisor Type

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

Use the **show module** command to display the type of supervisor module in the switch.

For a Supervisor-1 module, the output might look like this:

```
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
```

Send documentation comments to mdsfeedback-doc@cisco.com.

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

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

**Caution**

Migrating your supervisor modules is a disruptive operation.

**Note**

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

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

Configuring Generation 2 Switching Modules

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

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

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

For information on port index availability, refer to:

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

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

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

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

Upgrading Your Cisco MDS SAN-OS Software Image

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

- [Performing a Nondisruptive Software Upgrade on Generation 1 Modules, page 10](#)
- [Upgrading Your Version of Cisco Fabric Manager, page 11](#)
- [Upgrading with IVR Enabled, page 14](#)
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.1\(3a\), page 15](#)
- [Upgrading the SSI Image on Your SSM, page 16](#)
- [Upgrading a Switch with Insufficient Space for Two Images on the Bootflash, page 17](#)
- [Upgrading a Cisco MDS 9124 Switch, page 18](#)
- [Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch, page 18](#)



Caution

Before upgrading your Cisco MDS SAN-OS software image, you must run the Compact Flash Report utility described in the “[Managing System Hardware](#)” section of the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*. This reporting feature automatically scans your switch fabric and reports the status of Compact Flash on certain switch modules. To run this utility prior to upgrading your Cisco SAN-OS software image, upgrade Cisco Fabric Manager as described in the “[Upgrading Your Version of Cisco Fabric Manager](#)” section on page -11.

For instructions on how to scan your switch fabric and display the status of Compact Flash using CLI commands, refer to the “[Managing System Hardware](#)” section of the *Cisco MDS 9000 Family CLI Configuration Guide*.

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.
```

Send documentation comments to mdsfeedback-doc@cisco.com.

```
-- 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.

The caveat associated with this issue is CSCsm62295.

Upgrading Your Version of Cisco Fabric Manager

To upgrade your version of Cisco Fabric Manager, or install Cisco Fabric Manager for the first time, follow these steps:

-
- Step 1** Download **m9000-fm-3.1.3.jar** from the Software Center on Cisco.com (<http://www.cisco.com/cgi-bin/tablebuild.pl/mds-fm>). You must have a CCO account to access the files on Software Center.



Note As of Cisco MDS SAN-OS Release 3.1, Cisco Fabric Manager requires Java 1.5.

- Step 2** Launch the Fabric Manager installation program by doing one of the following:
- Navigate to the folder where you have downloaded the file and double-click it.
 - Open the file using Internet Explorer.
 - Enter **java -jar m9000-fm-3.1.3.jar** on the Windows or UNIX command line.
- Step 3** Select an installation folder for Fabric Manager on your workstation. The default location is C:\Program Files\Cisco Systems\MDS 9000 for Windows. On a Solaris or Linux machine, the installation path name is /usr/local/cisco_mds9000 or \$HOME/cisco_mds9000, depending on the permissions of the user performing the installation.



Note The Fabric Manager Server and the Fabric Manager Client must be able to communicate with each other at all times. They can be installed on different workstations or the same workstation.

- Step 4** Check the **Don't install and run FM Server** check box if you are installing just the Fabric Manager Client on a remote workstation.



Note For other methods and details on upgrading, downgrading, and uninstalling Cisco Fabric Manager, refer to the [Cisco MDS 9000 Family Fabric Manager Configuration Guide](#) and the [Cisco MDS 9000 Fabric Manager Quick Configuration Guide](#).

- Step 5** Click Finish to complete the Cisco Fabric Manager installation.

General Upgrading Guidelines

Use the following guidelines when upgrading to Cisco MDS SAN-OS Release 3.1(3a):

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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 18.
- 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 18.
- 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 5](#) for the nondisruptive upgrade path for all SAN-OS releases.
 - **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.
 - **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. 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 14 for these instructions.
 - **FICON:** If you have FICON enabled, the upgrade path is different. See [Table 6](#).

Use [Table 5](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.1(3a). Find the image release number you are currently using in the Current column of the table and use the path recommended.



Note

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

Table 5 Nondisruptive Upgrade Path to SAN-OS Release 3.1(3a)

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

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 5 Nondisruptive Upgrade Path to SAN-OS Release 3.1(3a) (continued)

| Current | Nondisruptive Upgrade Path |
|----------------|---|
| SAN-OS 2.1(2e) | You can nondisruptively upgrade directly to SAN-OS Release 3.1(3a). |
| SAN-OS 2.1(2d) | You can nondisruptively upgrade directly to SAN-OS Release 3.1(3a). |
| SAN-OS 2.1(2b) | You can nondisruptively upgrade directly to SAN-OS Release 3.1(3a). |
| SAN-OS 2.1(2) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.1(3a). |
| SAN-OS 2.1(1b) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.1(3a). |
| SAN-OS 2.1(1a) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.1(3a). |
| SAN-OS 2.0(x) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.1(3a). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.1(3a). |
| SAN-OS 1.x | Upgrade to SAN-OS Release 1.3(4a), then to Release 2.1(2b), and then upgrade to Release 3.1(3a). |

Use [Table 6](#) to determine your FICON nondisruptive upgrade path to Cisco MDS SAN-OS Release 3.1(3a). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.



Note

Cisco MDS SAN-OS Release 3.1(3a) is not FICON certified.

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 6 FICON Nondisruptive Upgrade Path to SAN-OS 3.1(3a)

| Current Release with FICON Enabled | Upgrade Path |
|------------------------------------|---|
| SAN-OS 3.0(2) | You can nondisruptively upgrade directly to SAN-OS Release 3.1(3a). |
| SAN-OS 2.0(2b) | Use the interface shutdown command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively upgrading from SAN-OS Release 2.0(2b) to SAN-OS Release 3.0(2), and then upgrade to Release 3.1(3a). An operationally down state includes <code>Link failure</code> or <code>not-connected</code> , <code>SFP not present</code> , or <code>Error Disabled</code> status in the output of a show interface command. When an interface is administratively shut it will then show as <code>Administratively down</code> . Interfaces that are currently up or trunking do not need to be shut down. |
| SAN-OS 1.x | Upgrade to SAN-OS Release 3.0(2). Use the interface shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively upgrading to Release 2.0(2b) and then upgrade to 1.3(4a). |

Upgrading with IVR Enabled

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

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

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

This issue was resolved in Cisco SAN-OS Release 2.1(2b); therefore, you must upgrade to Release 2.1(2b) before upgrading to Release 3.1(3a). 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 11](#). 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 **fdomain domain id static vsan vsan id** command to configure the static domains.



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

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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 syslogs for any ISL that was isolated.

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

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

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

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

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

- Step 7** Follow the normal upgrade guidelines for Release 2.1(2b). If you are adding new switches running Cisco MDS SAN-OS Release 2.1(2b) or later, upgrade all of your existing switches to Cisco SAN-OS Release 2.1(2b) as described in this workaround. Then follow the normal upgrade guidelines for Release 3.1(3a).



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 3.1(3a)

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 3.1(3a).

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

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

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

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

```
switch# show interface fc 2/1 - 32
fc2/1 is up
```

Send documentation comments to mdsfeedback-doc@cisco.com.

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

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

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

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

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

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

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

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

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

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

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

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](#).

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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 3.1\(3a\)](#)” section on page 15.
- The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** CLI command to determine your EPLD version. Refer to the [Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images](#) to upgrade your EPLD image.
- Refer to the [Cisco MDS Storage Services Module Interoperability Support Matrix](#) and the “[Managing Modules](#)” chapter in the [Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x](#), for information on upgrading your SSM.



Caution

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

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

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

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

The following MDS switches are affected by this issue:

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

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.

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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 3.1(3a) on a Cisco MDS 9124 Switch, follow these guidelines:

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

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

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

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

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

If you do not follow the upgrade path, (for example, you upgrade directly from SAN-OS Release 2.1(2b) to SAN-OS Release 3.1(3a)), 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:

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

- [General Downgrading Guidelines, page 19](#)
- [Downgrading the SSI Image on Your SSM, page 21](#)

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.1(3a):

- Install and configure dual supervisor modules.
- Issue the system **no acl-adjacency-sharing** execute command to disable acl adjacency usage on Generation 2 and Generation 1 modules. If this command fails, reduce the number of zones, IVR zones, TE ports, or a combination of these in the system and issue the command again.
- Disable all features not supported by the downgrade release. Use the **show incompatibility system downgrade-image** CLI command to determine what you need to disable.
- Layer 2 switching traffic is not disrupted when downgrading to Cisco SAN-OS Release 2.1(2) or later.
- Use the **show install all impact downgrade-image** CLI command to determine if your downgrade will be nondisruptive.
- Be aware that some features impact whether a downgrade is disruptive or nondisruptive:
 - **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively downgraded. See [Table 7](#) for the nondisruptive downgrade path for all SAN-OS releases.
 - **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during a downgrade. SSM Fibre Channel traffic is not.
 - **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. 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 14](#) for these instructions.
 - **FICON:** If you have FICON enabled, the downgrade path is different. See [Table 8](#).
 - **iSNS:** The iSNS feature does not support a graceful downgrade from Cisco MDS SAN-OS Release 3.1(3a) to any earlier SAN-OS release. Prior to a downgrade from Cisco SAN-OS 3.1(3a), disable the MDS iSNS server and remove all configurations associated with the MDS iSNS client.

Use [Table 7](#) to determine your nondisruptive downgrade path from Cisco SAN-OS Release 3.1(3a). Find the SAN-OS image you want to downgrade to in the To SAN-OS Release column of the table and use the path recommended.



Note

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

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 7 Nondisruptive Downgrade Path from SAN-OS Release 3.1(3a)

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

Use [Table 8](#) to determine your FICON 3.1(3a) nondisruptive downgrade path from Cisco SAN-OS Release 3.1(3a). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.



Note

Cisco MDS SAN-OS Release 3.1(3a) is not FICON certified.

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 8 FICON Downgrade Path from SAN-OS 3.1(3a)

| To SAN-OS Release with FICON Enabled | Downgrade Path |
|--------------------------------------|--|
| SAN-OS 3.0(2) | You can nondisruptively downgrade directly from SAN-OS Release 3.1(3a). |
| SAN-OS 2.0(2b) | Use the interface shutdown command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively downgrading from SAN-OS Release 3.1(3a) to SAN-OS Release 3.0(2), and then to SAN-OS Release 2.0(2b). An operationally down state includes <code>Link failure</code> or <code>not-connected</code> , <code>SFP not present</code> , or <code>Error Disabled</code> status in the output of a show interface command. When an interface is administratively shut it will then show as <code>Administratively down</code> . Interfaces that are currently up or trunking do not need to be shut down. |
| SAN-OS 1.3(4a) | Downgrade to SAN-OS Release 3.0(2). Use the shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively downgrading to Release 2.0(2b) and then downgrade to 1.3(4a). |

Downgrading the SSI Image on Your SSM

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

- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco SAN-OS Release 3.1(3a) 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.



Note

Following a downgrade from Cisco MDS SAN-OS Release 3.2(1) to an earlier SAN-OS release that does not support the Data Mobility Manager (DMM) feature that is offered from SAN-OS Release 3.2(1) onwards, you might have stale configuration information on the switch, if you had provisioned DMM on the SSM. In this situation, you can remove the stale configuration from the SSM by entering the

Send documentation comments to mdsfeedback-doc@cisco.com.

following commands:

```
switch(config)# poweroff module slot  
switch# purge module slot running-config
```

New Features in Cisco MDS SAN-OS Release 3.1(3a)

This section briefly describes the new features introduced in this release. For detailed information about the features listed, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.



Note

There are no new features in Cisco MDS SAN-OS 3.1(3a). The features described in this section were new as of Cisco MDS SAN-OS 3.1(3). For the complete Release 3.x documentation set, see the “[Related Documentation](#)” section on page 38.

New CompactFlash Test Capabilities

As of Cisco MDS SAN-OS 3.1(3), the ability to detect a faulty CompactFlash is built into the SAN-OS software. A new CompactFlash cyclic redundancy check (CRC) checksum test can check the state of the CompactFlash firmware on select modules. If the CompactFlash firmware is not corrupted, then the SAN-OS software can automatically update the CompactFlash firmware.

By default, the new CompactFlash CRC checksum test is enabled to automatically run in the background every seven days. New command-line interface (CLI) commands allow you to run the test on demand, change the automatic test interval, and disable the automatic testing.

The CompactFlash CRC checksum test can check if an affected CompactFlash is corrupted on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

If a CompactFlash is found to be corrupted, then the CRC checksum test is retried five times. If it fails five consecutive times, then the system initiates a failure action. The type of action depends on the module where the failure occurred:

Send documentation comments to mdsfeedback-doc@cisco.com.

- On a switching module, the system records a syslog event, logs an exception, and triggers a Call Home event. The module continues to run.
- On the standby supervisor, the system brings down the supervisor.
- On the active supervisor, if the hot standby supervisor is available, the system forces a switchover.
- On the active supervisor and on a single-supervisor system where there is no standby supervisor, the system records a syslog event, logs an exception, and triggers a Call Home event. The switch continues to run.

During a software upgrade to Cisco MDS SAN-OS 3.1(3a), all modules that are online are tested and the installation stops if any modules are running with a faulty CompactFlash. When this occurs, the switch cannot be upgraded until the situation is corrected. A system message displays the module information and indicates that you must issue the **system health cf-crc-check module** command to troubleshoot the problem.



Note

The new CompactFlash CRC checksum test feature is available only through the CLI; it cannot be used from Cisco Fabric Manager.

The Cisco Fabric Manager CompactFlash Check Utility that was included in previous Fabric Manager 3.1(x) releases, is not included in Cisco MDS SAN-OS Release 3.1(3).

For complete configuration information about the CompactFlash CRC checksum test feature, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#). For descriptions of new commands supported by the CompactFlash checksum feature, refer to the [Cisco MDS 9000 Family Command Reference](#).

System Default Port Mode F

As of Cisco SAN-OS Release 3.1(3), a new CLI command allows you to globally change the mode of Fibre Channel ports whose default mode is Auto, while avoiding traffic disruption caused by the formation of unwanted inter-switch links (ISLs). The new **system default switchport mode F** command sets the administrative mode of ports to mode F, while switch operation remains graceful. No ports are flapped.

This command changes the configuration to administrative mode F of the following ports:

- All ports that are down and that are not out-of-service.
- All F ports that are up, whose operational mode is F, and whose administrative mode is not F.

This command does not affect the configuration of the following ports:

- All user-configured ports, even if they are down.
- All non-F ports that are up; however, if non-F ports are down, this command changes the administrative mode of those ports.



Note

To ensure that ports that are part of ISLs do not get changed to port mode F, configure the ports in port mode E, rather than in Auto mode.

Send documentation comments to mdsfeedback-doc@cisco.com.

If you downgrade from Cisco MDS SAN-OS Release 3.1(3) to any earlier SAN-OS release after you execute the **system default switchport mode F** command, the ports retain the configuration that resulted from the execution of the command. In other words, the ports do not revert back to the mode they were in prior to executing the command. In addition, the **system default switchport mode F** command is not available in SAN-OS releases lower than Cisco SAN-OS Release 3.1(3a).

For additional information, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#) and the [Cisco MDS 9000 Family Command Reference](#).

Changes in SAN Device Virtualization

Cisco SAN-OS Release 3.1(3a) supports the following features of SAN Device Virtualization:

- Virtual initiators
- LUN zoning

For additional information, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#).

User Interface Changes in Cisco Fabric Manager

There are no changes in the user interface of Cisco Fabric Manager in Cisco SAN-OS Release 3.1(3a).

Fabric Manager Login Procedure

As of Cisco SAN-OS Release 3.1(1), logging into Fabric Manger is a two-part process that involves entering your username and password twice, in two different dialog boxes. To successfully complete the login process, you must:

- Log in to Fabric Manger Server by entering **admin** and **password** in the Fabric Manager Server dialog box
- Enter your username, password, and seed switch address in the Discover New Fabric dialog box and then open the fabric

To log in to Fabric Manger Server, follow these steps:

-
- Step 1** Double-click the Fabric Manager Client icon on your workstation.
 - Step 2** Enter **admin**, the default username, and **password**, the default password, in the Fabric Manager Server Login dialog box.
 - Step 3** Enter the the IP address of the FM Server or set it to it to **localhost** if you installed Fabric Manager Server on your local workstation.
 - Step 4** Click **Login**.
-

To discover new fabrics, follow these steps:

-
- Step 1** In the Discover New Fabric dialog box, enter the IP address of the Cisco MDS 9000 Family seed switch that you want Fabric Manager to use.
 - Step 2** Enter your username and password.

Send documentation comments to mdsfeedback-doc@cisco.com.

- Step 3** Choose the Auth-Privacy option MD5-DES (default) when you log in.
 - Step 4** Click **Discover**.
The Open Fabric dialog box displays.
 - Step 5** Check the check box(es) next to the fabric(s) you want to open in the Select column, or click **Discover** to add a new fabric.
 - Step 6** Click **Open** to open the fabric.
-

The password For additional information about logging in to Fabric Manager and setting the seed switch, refer to “Setting the Seed Switch in Cisco SAN-OS Release 3.1(1) and Later” in the [Cisco MDS 9000 Family Fabric Manager Configuration Guide](#).

Limitations and Restrictions

This section lists the limitations and restrictions for this release.

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 Cisco Fabric Switch for HP c-Class BladeSystem or Cisco Fabric Switch for IBM BladeCenter.

Interface Names on Cisco Fabric Switches and Interface Based Zoning

The Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter use different Fibre Channel interface names than those used on MDS 9000 Family switches. Interface names are used in many operations, including domain interface zoning.



Note

The Cisco Fabric Manager does not support using a port picker for configuring domain interface zoning for the Cisco Fabric Switch for IBM BladeCenter. You must enter the bay or ext interface name formats manually.

[Table 9](#) shows the mapping between the internal interface names and the displayed interface names on the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter to the displayed interface names.

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

Table 9 Cisco Fabric Switches - Mapping of Internal and Displayed Interface Names

| Cisco Fabric Switch for HP c-Class BladeSystem | | | Cisco Fabric Switch for IBM BladeCenter - | | |
|--|--------------------------|-------------|---|--------------------------|-------------|
| Internal Interface Name | Displayed Interface Name | Port Group | Internal Interface Name | Displayed Interface Name | Port Group |
| fc1/1 | ext8 | PortGroup 1 | fc1/1 | ext19 | PortGroup 1 |
| fc1/2 | bay6 | | fc1/2 | bay10 | |
| fc1/3 | bay13 | | fc1/3 | bay11 | |
| fc1/4 | bay5 | | fc1/4 | bay12 | |
| fc1/5 | ext7 | PortGroup 2 | fc1/5 | ext18 | PortGroup 2 |
| fc1/6 | bay14 | | fc1/6 | bay9 | |
| fc1/7 | bay15 | | fc1/7 | bay13 | |
| fc1/8 | bay7 | | fc1/8 | bay14 | |
| fc1/9 | bay4 | PortGroup 3 | fc1/9 | bay8 | PortGroup 3 |
| fc1/10 | ext1 | | fc1/10 | ext17 | |
| fc1/11 | bay3 | | fc1/11 | bay6 | |
| fc1/12 | bay11 | | fc1/12 | bay5 | |
| fc1/13 | bay12 | PortGroup 4 | fc1/13 | bay7 | PortGroup 4 |
| fc1/14 | ext2 | | fc1/14 | ext16 | |
| fc1/15 | bay2 | | fc1/15 | bay4 | |
| fc1/16 | bay1 | | fc1/16 | bay2 | |
| fc1/17 | bay10 | PortGroup 5 | fc1/17 | bay3 | PortGroup 5 |
| fc1/18 | ext3 | | fc1/18 | ext0 | |
| fc1/19 | bay9 | | fc1/19 | bay1 | |
| fc1/20 | ext4 | | fc1/20 | ext15 | |
| fc1/21 | bay16 | PortGroup 6 | | | |
| fc1/22 | bay8 | | | | |
| fc1/23 | ext6 | | | | |
| fc1/24 | ext5 | | | | |

Send documentation comments to mdsfeedback-doc@cisco.com.

CWDM SFPs

The 2-Gbps CWDM SFPs do not 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 3.1(3a) for Fabric Manager:

- You must download and install the Oracle Express database separately because Cisco Fabric Manager does not automatically install it. However, if you have Oracle installed on a PC, you should not install the Oracle Express database on the same PC because the installation will fail. In this instance, Fabric Manager must use the Hypersonic SQL database.
- 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, FM cannot detect NAT addresses. The timeout for URL connections is set for 500ms.

iSNS

Observe the following behaviors regarding the iSNS server and client:

- The iSNS feature does not support a graceful downgrade from Cisco MDS SAN-OS Release 3.1(3a) to any earlier SAN-OS release. Prior to a downgrade from Cisco SAN-OS 3.1(3a), disable the MDS iSNS server and remove all configurations associated with the MDS iSNS client.
- The Cisco MDS 9000 switches iSNS server does not support registration, query, or state change information from an actual iSCSI target.
- The iSNS client registers all targets outside the permitted VSAN if you configure the iSCSI interface and targets to be part of different VSANs.
- The iSNS client functionality on Cisco MDS 9000 switches does not work on VRRP interfaces.
- The iSNS client functionality on Cisco MDS 9000 switches does not support registration of iSLB initiators.

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.

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

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 3.1\(3a\)”](#) section on page 15.

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.

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 10](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 10 *Open Caveats and Resolved Caveats Reference*

| DDTS Number | Software Release (Open or Resolved) | |
|----------------------------|-------------------------------------|---------|
| | 3.1(3) | 3.1(3a) |
| Severity 1 | | |
| CSCsi92509 | O | R |
| CSCsj49207 | O | O |
| Severity 2 | | |
| CSCsg49151 | O | O |
| CSCsi49231 | O | O |
| CSCsi72048 | O | O |
| CSCsi77398 | O | O |
| CSCsi78480 | O | O |
| CSCsi79146 | O | R |
| CSCsi80055 | O | R |
| CSCsj04224 | O | R |
| CSCsj14140 | O | O |
| CSCsj19105 | O | R |
| CSCsj64048 | O | O |
| CSCsj65565 | O | O |
| CSCsj72662 | – | O |
| CSCso72230 | O | O |
| Severity 3 | | |
| CSCin95789 | O | O |
| CSCsd21187 | O | O |
| CSCse31881 | O | O |
| CSCsg19148 | O | O |
| CSCsg19303 | O | O |
| CSCsg62704 | O | O |
| CSCsh05721 | O | O |
| CSCsh63658 | O | O |
| CSCsh70152 | O | O |
| CSCsi51436 | O | O |
| CSCsi56949 | O | O |
| CSCsi77055 | O | R |

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 10 Open Caveats and Resolved Caveats Reference (continued)

| DDTS Number | Software Release (Open or Resolved) | |
|----------------------------|-------------------------------------|---------|
| | 3.1(3) | 3.1(3a) |
| CSCsj07363 | O | R |
| CSCsj13175 | O | O |
| CSCsj26584 | O | R |
| CSCsj29134 | O | O |
| CSCsj50299 | – | O |
| CSCsj52389 | O | O |
| CSCsj95379 | O | O |
| CSCsk21652 | O | O |
| CSCsk48149 | O | O |
| CSCso63465 | O | O |
| Severity 4 | | |
| CSCsh68830 | O | O |
| CSCsi79423 | O | R |
| CSCsi87114 | O | R |
| CSCsi98091 | O | R |
| CSCsj44453 | O | O |
| Severity 6 | | |
| CSCeh35635 | O | O |

Resolved Caveats

- [CSCsi92509](#)
Symptom: If you are running Cisco MDS SAN-OS Release 3.1(2b) and you are using FCIP tape acceleration, you may experience intermittent FCIP link flaps.
Workaround: This issue is resolved.
- [CSCsi79146](#)
Symptom: A virtual initiator is configured with the host's port world wide name (pWWN), and the virtual initiator and virtual target logical unit numbers (LUNs) are zoned in the active zone set. When you issue the **show incompatibility system bootflash:** command, the switch does not display the incompatibility.
Workaround: This issue is resolved.
- [CSCsi80055](#)
Symptom: If you upgrade a system with a modem configuration to Cisco MDS SAN-OS Release 3.x, the upgrade fails and the system reboots.
Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com.

- CSCsj04224

Symptom: If you install a feature license on any module, then the storage services module (SSM) with the SCSI flow feature will be reprovisioned and write acceleration on the flows will be affected.

Workaround: This issue is resolved.
- CSCsj19105

Symptom: A crash might occur in the intelligent line card (ILC) helper process when provisioning or deprovisioning a storage application on the SSM card.

Workaround: This issue is resolved.
- CSCsi77055

Symptom: An MDS switch that provides IVR routing on a local VSAN may not be able to export new devices via IVR if there are multiple IVR routers in the local VSAN or if one IVR router contains stale entries for a device. When an IVR router has stale information, it will be out of sync with the other IVR routers. Because IVR routers work in sync, then IVR cannot export any new devices.

Workaround: This problem is resolved.
- CSCsj07363

Symptom: An SNMP Get-Next Request for the MIB object `ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex` on an MDS 9000 switch resolves by asking `ifIndex` for a loopback address. Because there is no hardware (`ifIndex`) for a loopback address, the `ifIndex` reply for this interface is skipped and the next possible instance of the object, which is `IP-MIB::ipAdEntNetMask`, is returned.

Workaround: This issue is resolved.
- CSCsj26584

Symptom: When Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is enabled, NAS-IP is not sent. When Password Authentication Protocol (PAP) is used, NAS-IP is sent. PAP is the default authentication protocol.

Workaround: This issue is resolved.
- CSCsi79423

Symptom: If you disable error or discard messages in Performance Manager via the `server.properties` file, you may see the following error in the `FMServer.log` file:

```
WARNING 2007/05/07 14:54:26 PM 10.62.40.75 error: java.io.EOFException
java.io.EOFException
  at java.io.RandomAccessFile.readChar(RandomAccessFile.java:683)
  at com.cisco.dcbu.lib.rrd.core.RrdFile.readString(Unknown Source)
  at com.cisco.dcbu.lib.rrd.core.RrdString.get(Unknown Source)
  at com.cisco.dcbu.lib.rrd.core.RrdString.get(Unknown Source)
  at com.cisco.dcbu.lib.rrd.core.Header.<init>(Unknown Source)
  at com.cisco.dcbu.lib.rrd.core.RrdDb.<init>(Unknown Source)
  at com.cisco.dcbu.pm.Query.getErrDB(Unknown Source)
  at com.cisco.dcbu.pm.PmStore.store(Unknown Source)
  at com.cisco.dcbu.pm.PmStore.run(Unknown Source)
  at java.lang.Thread.run(Thread.java:595)
```

In addition, a file whose filename is a WWN will be erroneously created in the Performance Manager database.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com.

- CSCsi87114
Symptom: When you enter the **show fcip tape-session** command, the switch displays the outputs of the first ten sessions, but additional session outputs are needed.
Workaround: This issue is resolved.
- CSCsi98091
Symptom: If you attempt to examine the logging information of an FCIP tunnel that has write acceleration enabled, you might notice that some of the logs do not contain the correct debugging information. The logging information can be used to debug possible error conditions in an FCIP tunnel.
Workaround: This issue is resolved.

Open Caveats

- CSCsj49207
Symptom: An FCIP link running tape acceleration may flap and dump its core when a malfunctioning host repeatedly asks for a status from the tape.
Workaround: Shut down the malfunctioning host switch.
- 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.
- 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: 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.
- 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)
```

Send documentation comments to mdsfeedback-doc@cisco.com.

- Workaround:** If both ends of an FCIP link are not on an MPS-14/2 module, do not use mode 1 and auto.
- CSCsi77398

Symptom: Backups of IBM Tivoli Storage Manager (TSM) running AIX might fail when using FCIP tape acceleration if the tape sends an end-of-tape status while FCIP tape acceleration has partially buffered write commands.

Workaround: Disable FCIP tape acceleration.
 - 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: None.
 - CSCsj14140

Symptom: FCIP links running read acceleration might fail in certain circumstances due to a defect in error handling.

Workaround: Disable FCIP tape acceleration.
 - 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: Statically define the DVTs using the **santap module** command, as in the following example:

```
switch(config)# santap module slot-number dvt target-pwvn target-pwvn target-vsan
target-vsan-id dvt-name dvt-name dvt-vsan dvt-vsan-id lun-size-handling 1
```
 - CSCsj65565

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

Workaround: Add the company OUI ID to the switch database so that the switch can assign unique area IDs to the Spectra Logic tape drives.
 - 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: %$V$SAN 4094%$ Interface fc4/16 is down (Hardware Failure)
%PORT-5-IF_DOWN_HW_FAILURE: %$V$SAN 4094%$ Interface fc4/15 is down (Hardware Failure)
%PORT-5-IF_DOWN_HW_FAILURE: %$V$SAN 1003%$ Interface fc4/14 is down (Hardware Failure)
```

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

Send documentation comments to mdsfeedback-doc@cisco.com.

```

===== EXCEPTION LOG =====
*** Log# 0 ***
Device Id : 7
Device Name : aladdin
Device Error Code : c0703572(H)
Sys Error : Q-Engine instance shutdown
Errrtype : 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: Reload the affected module using the **reload module slot** command, or remove and reinsert the module to recover the affected ports.

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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.
- 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.
- 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.
- 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: After you replace the bootflash and the standby supervisor boots up, issue the **copy running-config startup-config** command to synchronize the configuration from the active supervisor to the standby supervisor.
- 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: None.
- 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: None.

Send documentation comments to mdsfeedback-doc@cisco.com.

- CSCsh70152

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

Workaround: None. 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.
- 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: From Fabric Manager Server, close the fabric and then re-open it without checking the **Accelerate Discovery** check box on the the Discover New Fabric dialog box.
- 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: Either create the VSAN using static domain IDs, or use the CLI to create new VSANs at different times.
- 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: To put the module back in service, enter the commands shown in this example:

```
switch(config)# poweroff module slot-number
switch# purge module slot-number running-config
switch(config)# no poweroff module slot-number
```

Configure the module again because the previous configuration will be lost.
- 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: Reload the module, or contact Cisco TAC for a less disruptive workaround.
- CSCsj50299

Symptom: Following an upgrade to Cisco SAN-OS 3.1(3a), the SSH server stops working correctly if RSA1 keys are configured. As a result of CSCsj50299, the standby supervisor in an MDS 9500 Series switch may fail to fully boot after attempting an upgrade from Cisco SAN-OS 3.1(3a).

Workaround: Remove the configured RSA1 keys.
- 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: None.

Send documentation comments to mdsfeedback-doc@cisco.com.

- 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: None.
- CSCsk21652
Symptom: If the tape sends a certain error status without requesting status confirmation, the FCIP link may flap.
Workaround: Disable FCIP tape acceleration.
- 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: None.
- 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.
- 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: None.
- CSCsj44453
Symptom: Following an upgrade, a device might be incorrectly imported to a non-native VSAN.
Workaround: Shut down and then re-enable the host's port on the switch before importing the device.
- 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.

[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. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at this URL:

http://www.cisco.com/en/US/customer/products/ps5989/products_documentation_roadmap09186a00804500c1.html

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:

<http://www.ibm.com/storage/support/2062-2300/>

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 SVC Releases*
- *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 IBM SAN Volume Controller Software for Cisco MDS 9000*
- *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 MDS 9020 Fabric Switch Hardware Installation Guide*

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*

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

- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*
- *Cisco MDS 9000 Family Fabric Manager Database Schema*

Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch 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 Fibre Channel X2 Transceiver Module Installation Note*

Send documentation comments to 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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, 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. (0809R)

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.