

Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.0(3)

Release Date: January 6, 2005

Text Part Number: OL-6249-03 Z0

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 25](#).



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 On-Line History Change

Revision	Date	Description
A0	1/06/2005	Created release notes
B0	1/14/2005	Removed DDTS CSCeg01545. This bug was resolved in a previous release. Added DDTS CSCeg56197 .
C0	2/23/2005	Added information to the Limitations and Restrictions section. Added DDTS CSCeg85146 and CSCin81851
D0	3/15/2005	Added CSCed20053 , CSCeh21199 , CSCef95611 , and CSCef56229
E0	03/24/2005	Added DDTS CSCeg61535 .
F0	04/12/2005	Removed DDTS CSCeg07339 Added DDTS CSCeh49026 , CSCeh44216 , CSCeh51924 ,
G0	04/13/2005	Added DDTS CSCeg81089
H0	05/03/2005	Added DDTS CSCeg82721 and CSCeh65824



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

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

Table 1 On-Line History Change (continued)

Revision	Date	Description
I0	5/19/2005	Removed DDTS CSCeh44216
J0	5/24/2005	Added DDTS CSCeg66225 and CSCeh42252
K0	5/31/2005	Added DDTS CSCeh96928
L0	06/01/2005	Added DDTS CSCeg24199
M0	06/23/2005	Added DDTS CSCei25319
N0	08/02/2005	Added DDTS CSCed57251 , CSCeh61610 , CSCeh64080 , CSCec31365 , CSCeg20932 , CSCeg53114 , CSCeg66225 , CSCeh19639 , CSCeh52280 , CSCeh56143 , CSCeh82490 , CSCeh83514 , CSCeh87985 , CSCeg90336 , CSCeh52973 , CSCeh87930 , CSCeh90270 , CSCeh93625 , CSCei01431 , CSCeh73101 , and CSCei29086
O0	08/05/2005	Added DDTS CSCeh41099
P0	08/22/2005	Removed DDTS CSCeh61610
Q0	08/23/2005	Added DDTS CSCeh61610
R0	12/07/2005	Added DDTS CSCsc31424
S0	12/30/2005	Added DDTS CSCei91968
T0	05/02/2006	Removed DDTS CSCeh52973 Added DDTS CSCeg33121 , CSCsd29338 , CSCei57342 , CSCei58652 , CSCei67982 , CSCei91676 , CSCsc09732 , CSCsc33788 , and CSCsd83775
U0	06/06/2006	Removed DDTS CSCed16845
V0	9/05/2006	Added DDTS CSCsd78967
W0	9/13/2006	Added DDTS CSCsf21970
X0	11/07/2006	Added DDTS CSCsg15392
Y0	02/23/2007	Added DDTS CSCse99087 , CSCsg03171 , and CSCsh27840 .
Z0	08/24/2007	Modified the description of DDTS CSCsd83775 .

Contents

This document includes the following sections:

- [Introduction, page 3](#)
- [System Requirements, page 3](#)
- [Image Upgrade, page 6](#)
- [New Features in Cisco MDS SAN-OS Release 2.0\(3\), page 7](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 12](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation, page 26](#)

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

- [Documentation Feedback, page 27](#)
- [Cisco Product Security Overview, page 27](#)
- [Obtaining Technical Assistance, page 28](#)
- [Obtaining Additional Publications and Information, page 30](#)

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offers intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. These switches combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 2.0(3) and includes the following topics:

- [Components Supported, page 3](#)
- [Determining the Software Version, page 6](#)

Components Supported

[Table 2](#) lists the software 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	Not orderable	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	Not orderable	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	Not orderable	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only

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

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

Component	Part Number	Description	Applicable Product
License	M9500ENT1K9	Enterprise package	MDS 9500 Series
	M9200ENT1K9	Enterprise package	MDS 9200 Series
	M9100ENT1K9	Enterprise package	MDS 9100 Series
	M9500FIC1K9	Mainframe package	MDS 9500 Series
	M9200FIC1K9	Mainframe package	MDS 9200 Series
	M9100FIC1K9	Mainframe package	MDS 9100 Series
	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 ASM or SSM
M9200SSE1K9	Storage services enabler package	MDS 9200 series with ASM or SSM	
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs ¹ 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-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 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

[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
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I, module.	MDS 9500 Series only
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).	
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage Services module.	
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage Services module.	
	DS-X9032-SMV	32-port Fibre Channel Advanced Services Module (ASM).	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM)	
	DS-X9560-SMC	Caching Services Module (CSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
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.	
CWDM ²	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 1-Gbps/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s).	
Power supplies	DS-CAC-300W	300-W ³ AC power supply.	MDS 9100 Series only
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC 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.	
CompactFlash	MEM-MDS-FLD512 M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family

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

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

Determining the Software Version



Note

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

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

To determine the version of the 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.

Image Upgrade

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.

You can nondisruptively upgrade to Cisco MDS SAN-OS Release 2.0(3) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of SAN-OS, upgrade to Release 1.3(x) and then Release 2.0(3).

When downgrading from Cisco MDS SAN-OS Release 2.0(3) to Release 1.3(x), you might need to disable new features in Release 2.0(3) for a nondisruptive downgrade. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade enables the compatibility check. The check indicates that the downgrade is disruptive and the reason is “current running-config is not supported by new image”.

```
Compatibility check is done:
Module  bootable      Impact  Install-type  Reason
-----  -
      2      yes      disruptive      reset  Current running-config is not
supported by new image
      3      yes      disruptive      reset  Current running-config is not
supported by new image
      5      yes      disruptive      reset  Current running-config is not
supported by new image
      6      yes      disruptive      reset  Current running-config is not
supported by new image
```

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 Configuration Guide* for more details.

Send documentation comments to mdsfeedback-doc@cisco.com

New Features in Cisco MDS SAN-OS Release 2.0(3)

There are no new features introduced in Release 2.0(3).



Note

These release notes are specific to this release. For the Cisco MDS SAN-OS Release 2.x documentation set, see the [“Related Documentation”](#) section on page 25.

Limitations and Restrictions

The following limitations and restrictions apply to all switches in the Cisco MDS 9000 Family:

- [Upgrading to Cisco MDS SAN-OS Release 2.0\(3\) from Release 1.3\(4a\)](#), page 7
- [Temporary User Account](#), page 10
- [Deleting Roles](#), page 10
- [The localizedkey Option](#), page 10
- [Extended BB_Credit Support](#), page 10
- [DPVM](#), page 10
- [PortChannel Autocreation](#), page 11
- [IP-ACL Support](#), page 11
- [Port Mode for IBM FAStT 500 Storage System](#), page 11
- [FCIP Links](#), page 11
- [Fabric Manager/Device Manager Support on Windows2003](#), page 11

Upgrading to Cisco MDS SAN-OS Release 2.0(3) from Release 1.3(4a)

This procedure applies to Fabric Manager and Device Manager applications using Cisco MDS SAN-OS Release 1.3(4a) software.

To upgrade a switch from 1.3(4a) to 2.0(3), use Device Manager to copy the image files to bootflash and then use Fabric Manager to perform the upgrade.

To copy the image files from a server or PC to bootflash, follow these steps:

-
- Step 1** Start TFTP, FTP, SCP, or SFTP on the server or PC where you have the image files stored.
 - Step 2** In Device Manager, select **Admin > Flash Files**. You see the bootflash directory listed for the supervisor’s local partition, by default.
 - Step 3** Select the device and partition from the drop-down lists for the directory containing the file you want to copy.
 - Step 4** Click the **Copy** button to open the Copy dialog box.
 - Step 5** Select the protocol you want to use to perform the copy procedure.
 - Step 6** Enter the address of the source server.
 - Step 7** If necessary, enter your remote username and password on that server.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 8 Click the ... button after the SourceName field to browse for the source file on your local PC or on the server, depending on the type of copy.

Step 9 Enter the destination name for the file.



Note If you are copying to Flash, the file name must be of the form
[device:][<partition>:<file>

where <device> is a value obtained from the Flash device name,
<partition> is obtained from the Flash partition name
and <file> is any character string that does not have embedded colon characters.

Step 10 Click **Apply**.

Send documentation comments to mdsfeedback-doc@cisco.com

To upgrade using Fabric Manager, use the Software Install Wizard. Software upgrades may be disruptive under the following conditions:

- A single supervisor system with kickstart or system image changes.
- A dual supervisor system with incompatible system software images.



Note Before you use the Software Install Wizard, verify that the standby supervisor management port is connected.

To use the Software Install Wizard, follow these steps:

-
- Step 1** Open the Software Install Wizard by clicking on its icon in the toolbar.
You see the Software Install Wizard.
- Step 2** Select the switches that you want to upgrade or install images from the displayed list.
You must select at least one switch to proceed. When finished, click **Next**.
- Step 3** Specify the new images to use for each switch model.
To use images that are already downloaded (the file is already on the bootflash), check the **Skip Image Download** check box.
- Step 4** Double-click the table cell under System, Kickstart, or Asm-sfn to see a drop-down list of images to choose from.
- Step 5** Select an image to use for the upgrade.
You must select at least one image for each switch to proceed.



Note There is no limit to the number of switches you can upgrade. However, the upgrade is a serial process; that is, only a single switch is upgraded at a time.

- Step 6** Start the upgrade.
If you check **version check** before the upgrade process is started, a version check is done. This check provides information about the impact of the upgrade for each module on the switch. It also shows any HA-related incompatibilities that might result. You see a final dialog box at this stage, prompting you to confirm that this check should be performed.



Caution If **version check** is enabled, the upgrade will proceed even if your version is newer than the version you are installing.



Note Before exiting the session, be sure the upgrade process is complete. The wizard will display a status as it goes along. Check the lower left-hand corner of the wizard for the status message `Upgrade Finished`. First, the wizard displays the message `Success` followed a few seconds later by `InProgress Polling`. Then the wizard displays a second message `Success` before displaying the final `Upgrade Finished`.

Refer to the *Cisco MDS 9000 Fabric Manager Guide*.

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

Temporary User Account

When you log in to a Cisco MDS switch successfully using the Fabric Manager or Device Manager through Telnet or SSH and if that switch is configured for AAA server-based authentication, a temporary SNMP user entry is automatically created with an expiry time of one day. The switch authenticates the SNMPv3 protocol data units (PDUs) with your Telnet/SSH login name as the SNMPv3 user are authenticated by the switch. The management station can temporarily use the Telnet/SSH login name as the SNMPv3 `auth` and `priv` passphrase. This temporary SNMP login is only allowed if you have one or more active MDS shell sessions. If you do not have an active session at any given time, your login is deleted and you cannot perform SNMP v3 operations.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Deleting Roles

If a user only belongs to one of the newly-created roles and that role is subsequently deleted, then the user immediately defaults to the network-operator role.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

The localizedkey Option

Avoid using the **localizedkey** option when configuring an SNMP user from the CLI. The localized keys are not portable across devices as they contain device engine ID information. If a configuration file is copied to the device, the passwords may not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device. Passwords specified with the **localizedkey** option are limited to a 130 characters.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Extended BB_Credit Support

The last two Fibre Channel ports (port 13 and port 14) and the two Gigabit Ethernet ports in the MPS-14/2 module and in the Cisco MDS 9216i Switch do not support the extended BB_credits feature.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

DPVM

The DPVM feature overrides any existing static port VSAN membership configuration. If a device is not configured for a specific VSAN, it continues to be part of the existing port VSAN.

If the VSAN corresponding to the dynamic port is deleted or suspended, the port is shut down.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

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

PortChannel Autocreation

When enabling autocreation, we recommend that you retain at least one interconnected port between the switches without any autocreation configuration. If all ports between two switches are configured with the autocreation feature at the same time, you may face a possible traffic disruption between these two switches as the ports are automatically disabled and reenabled when ports are added to an autocreated PortChannel.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

IP-ACL Support

Do not apply IP-ACLs to only one member of a PortChannel group. Apply IP-ACLs to the entire channel group.

If IP-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

Port Mode for IBM FAStT 500 Storage System

If you are connecting IBM FAStT 500 storage system to Cisco MDS switches, configure the port mode as F instead of Fx or Auto.

Refer to the *Cisco MDS 9000 Family Configuration Guide*.

FCIP Links

If the FCIP write acceleration feature or the FCIP compression feature is enabled on an FCIP link, then switches in a fabric running Cisco MDS SAN-OS Release 1.3 will not be compatible with switches in the same fabric running Cisco MDS SAN-OS Release 2.0(3).

If a Cisco MDS switch running Cisco MDS SAN-OS Release 1.3 is upgraded to Cisco MDS SAN-OS Release 2.0(3) when FCIP compression or write acceleration is enabled, then an FCIP link failure will occur.

If the upgrade is performed using the Fabric Manager, then the FCIP link continues to remain in the failed state till the connected switches are upgraded.

To avoid this FCIP link failure, disable the write acceleration and the FCIP compression features before beginning the upgrade process.

Fabric Manager/Device Manager Support on Windows2003

Fabric manager/Device manager does not work properly with JRE version 1.4.2_03 on Windows 2003 operating system.

JRE version 1.4.2_05 has been found to work without any issues on Windows 2003.

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

Table 3 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release (Open or Resolved)	
	2.0(2b)	2.0(3)
Severity 1		
CSCeg33121	O	O
CSCsd29338	O	O
Severity 2		
CSCed57251	O	O
CSCeg11095	O	O
CSCeg12962	O	O
CSCeg20932	O	O
CSCeg53094	O	R
CSCeg53114	O	O
CSCeg58996	O	R
CSCeg82721	O	O
CSCeg90336	O	O
CSCeh49026	O	O
CSCeh61610	O	O
CSCeh87930		O
CSCeh90270		O
CSCeh93625		O
CSCeh96928	O	O
CSCei01431		O
CSCei25319	O	O
CSCsd78967	O	O
CSCsh27840	O	O
Severity 3		
CSCec31365	O	O
CSCed14920	O	O
CSCed20053	O	O
CSCef56229	O	O
CSCef95611	O	O
CSCeg01551	O	O
CSCeg12383	O	O

Send documentation comments to mdsfeedback-doc@cisco.com

Table 3 Release Caveats and Caveats Corrected Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.0(2b)	2.0(3)
CSCeg24199	O	O
CSCeg35694	O	O
CSCeg37200	O	O
CSCeg37598	O	O
CSCeg40856	O	O
CSCeg56197	O	O
CSCeg59198	O	R
CSCeg61535	O	O
CSCeg66225	O	O
CSCeg81089	O	O
CSCeg85146	O	O
CSCeh19639	O	O
CSCeh21199	O	O
CSCeh41099	O	O
CSCeh51924	O	O
CSCeh52280	O	O
CSCeh56143	O	O
CSCeh64080	O	O
CSCeh65824	O	O
CSCeh73101		O
CSCeh82490	O	O
CSCeh83514	O	O
CSCeh87985	O	O
CSCei29086		O
CSCei57342		O
CSCei58652		O
CSCei67982	O	O
CSCei91676	O	O
CSCei91968	O	O
CSCin81851	O	O
CSCin84860	O	R
CSCsc09732		O
CSCsc31424	O	O
CSCsc33788	O	O
CSCsd83775		O

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

Table 3 Release Caveats and Caveats Corrected Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.0(2b)	2.0(3)
CSCse99087	O	O
CSCsf21970	O	O
CSCsg03171	O	O
CSCsg15392		O
Severity 4		
CSCeh42252	O	O

Resolved Caveats

- [CSCeg53094](#)
Symptom: The XIOTECH initiator does not recognize remote storage devices.
Workaround: Issue the **fcid-allocation area company-id 0x00d0b2** command before connecting the devices to the switch to ensure that the storage devices get FCIDs with a unique area byte. If the devices are already connected, refer to the *Cisco MDS 9000 Family Configuration Guide* for information about adding a company-id to the list.
- [CSCeg58996](#)
Symptom: Scheduled jobs are sometimes executed twice in a day.
Workaround: None. Upgrade to Cisco MDS SAN-OS Release 2.0(3)
- [CSCeg59198](#)
Symptom: If your host or management application is configured to receive notifications from a Cisco MDS 9000 Family switch using SNMPv1, the source address of the notification might not contain the IP address of the switch. As a result, the host may not interpret the notification properly.
Workaround: Use SNMPv2c or upgrade to Cisco MDS SAN-OS Release 2.0(3).
- [CSCin84860](#)
Symptom: A null pointer exception error message might occur after zone merge failure recovery in Fabric Manager.
Workaround: Close the dialog box and relaunch it.

Open Caveats

- [CSCeg33121](#)
Symptom: A small amount of memory in the IP configuration process leaks each time any of the following commands execute: **show running-config**, **show startup-config**, **copy running-config startup-config**. After repeated occurrences, the command fails to execute.
Workaround: None.
- [CSCsd29338](#)

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

Symptom: The port manager might crash and a switchover might occur when FICON is configured and the MDS switch is interoperating with a CNT device. This occurs when a port is UP, a link failure happens, and the remote node ID (RNID) retry timer is activated.

Workaround: None

- CSCed57251

Symptom: In some rare instances in Cisco MDS SAN-OS Release 1.3, 2.0, and 2.1(1), when the IP Storage Services (IPS) module restarted after a failure, VSAN membership information about iSCSI interfaces was lost. However, a configuration saved with the **copy running-config startup** command was not lost.

Workaround: None.

- CSCeg11095

Symptom: Duplicate fabrics are opened under different SANs when the loadFromDB option is selected.

Workaround: Select **Admin > Fabrics** to remove the fabric, and then reopen it with the loadFromDB box deselected.

- CSCeg12962

Symptom: Some hosts may not accept IKE tunnel creation from Cisco MDS 9000 Family switches when an IKE session already exists in the switch. In such cases it may take more than the expected time for the IPsec session to come up. This scenario can happen when the Gigabit Ethernet interface on the switch fails and comes back up or if you issue a VRRP switchover to a different switch.

Workaround: For a faster recovery, disconnect and reinitiate the iSCSI session from the host.

- CSCeg20932

Symptom: If an IPS module with operational FCIP PortChannels is reloaded, upgraded, or downgraded, the supervisor module may be reloaded causing the system to reboot.

Workaround: Before reloading, upgrading, or downgrading an IPS module, shut down all FCIP PortChannels on the line card.

- CSCeg53114

Symptom: WWNs assigned to iSCSI initiators by the system can inadvertently be returned to the system when an upgrade fails or a manual downgrade is performed, such as when an older iSAN software version is booted up without using the **install all** command. In these scenarios, the system can later assign those WWNs again to other initiators, which causes conflicts. This bug is a duplicate of CSCei17870.

- CSCeg82721

Symptom: Under certain traffic patterns, the Gigabit Ethernet port can flap when auto compression mode is selected. This problem can also occur rarely even when compression mode 1 is selected.

Workaround: Use mode 2 or mode 3 compression mode if the maximum throughput required is less than 25 Mega bits/sec. There is no workaround if the throughput requirement is > 25 Mbps.

- CSCeg90336

Symptom: A user that you create in Fabric Manager or Device Manager cannot log in from the console. Release 2.1(2) fixes this problem. However, if a third-party application creates a user using SNMP, a new MIB is required for Release 3.0.

Workaround: Third-party applications should use SSH to connect to the MDS 9000 switch, and then use CLI commands to create the user account.

- CSCeh49026

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

Symptom: The application might report that the loop port is not up, however, the port is online and operational.

Workaround: Issue the shutdown/no shutdown command sequence to clear the problem.

- CSCeh61610

Symptom: FCIP Write Acceleration does not work with certain storage replication subsystems.

Workaround: None.

- CSCeh87930

Symptom: A newly configured FCIP link may fail to come up when running on an MPS-14/2 module. This symptom may occur following an upgrade of Cisco MDS SAN-OS Release 2.0(1b) to Release 2.0(3) and the configuration of a new FCIP link.

In the log on the switch, you may see the following messages:

```
%PORT-5-IF_DOWN_ELP_FAILURE_ISOLATION: %$VSAN xyz%$ Interface fcipabc is down
(Isolation due to ELP failure)
%PORT-5-IF_DOWN_OFFLINE: %$VSAN xyz%$ Interface fcipabc is down (Offline)
%PORT-5-IF_DOWN_NONE: %$VSAN xyz%$ Interface fcipabc is down (None)
```

VSAN xyz is the allowed VSAN number for the FCIP interface and interface fcipabc is the configured FCIP interface number.

Workaround: Reload the MPS-14/2 module using the **reload module *module-number*** command, where *module-number* is a specific module.

- CSCeh90270

Symptom: Two MDS 9000 switches configured with an FCIP bridge port (B port) tunnel may have problems with multi-frame sequences. You may notice this problem activating large zone sets when the SFC frame times out.

Workaround: If the connection is between two MDS switches, then the B port configuration is not required and should not be used. If B port is a requirement, then reduce the zone set length by not distributing the full database, or use VSANs.

- CSCeh93625

Symptom: The line cards shut down after the supervisor module fails.

Workaround: Remove the failed supervisor module and reinsert the line card. Or enter the **no poweroff module *slot*** command in Exec mode on the switch, where *slot* is the slot number of the module that failed.

- CSCeh96928

Symptom: If your switch port is configured in auto speed (switchport speed auto) and auto mode (switchport mode auto), the switch-port fails to establish a link with the device connected through Emulex HBA LP8000 and remains in link-failure state. The problem occurs with the following combination of HBA, Driver, Firmware, and OS configured at 1 Gbps.

Workaround: Configure the switch port speed to 1 Gbps (switchport speed 1000) to support the Emulex HBA LP8000.

- CSCei01431

Symptom: An FCIP interface stays in the initializing state if it is part of a PortChannel and it is removed with the **no fcip enable** command.

Workaround: Remove the PortChannel that the FCIP interface previously belonged to.

- CSCei25319

Send documentation comments to mdsfeedback-doc@cisco.com

- Symptom:** An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to a SNMP query. In some cases, this results in the query not being responded to.

Workaround: Perform a refresh on Device Manager to clear the problem.
- CSCsd78967

Symptom: If you remove a port from a port channel or shutdown a member port of a port-channel, the ConnUnitPortStatus/State trap is not sent.

Workaround: None.
- CSCsh27840

Symptom: While using an FCIP link for remote SPAN, it is possible that the FCIP link may flap.

Workaround: Do not use FCIP links for Remote SPAN.
- CSCec31365

Symptom: When IVR is enabled, the Fabric-Device Management Interface information is not transferred across VSANs for IVR devices.

Workaround: None.
- CSCed14920

Symptom: During a switch upgrade, a SAN Volume Controller (SVC) node may not save its entire state under rare circumstances. This results in that node not being part of the cluster after the switch upgrade. Verify this symptom by issuing the **show nodes local** command at the `svc-config` prompt—the command output displays the following information:

 - The `cluster state` of the affected SVC node is `unconfigured`.
 - The `node state` of the affected SVC node is `free`.

Workaround: Manually remove the SVC node from the cluster and then add the node back into the cluster. Refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for procedural details.
- CSCeh19639

Symptom: Alias for a down endport is not shown and is referenced by its pwwn in the Edit FullZoneset screen of the Fabric Manager rather than the fcalias name. This does not affect the functionality of adding those members to the zones either in Fabric Manager or in the CLI.

Workaround: None
- CSCeh73101

Symptom: When you perform a nondisruptive upgrade from Release 1.3(x) to 2.0(x), and then issue the **show running-config** command, the switch displays the wrong user. The user shown will be inconsistent with the user shown when you issue the **show user-account** command.

Workaround: Recreate the user.
- CSCed20053

Symptom: On rare occasions, the **install license** command may fail due to the saved state of the switch configuration. This may occur after saving a remote configuration to the switch using the **copy remote-url start-up** command.

Workaround: Issue the **copy ru st** command. The **install license** command should work properly after that.
- CSCef56229

Send documentation comments to mdsfeedback-doc@cisco.com

Symptom: If an iSCSI initiator is configured differently on multiple switches, iSNS might report more targets to the initiator than the initiator can access. An iSCSI initiator would get a target error if it attempts to establish a connection.

Workaround: None.

- CSCef95611

Symptom: After a successful database merge, the show **cfs merge status name** *application_name* command output may not reflect the correct merge status. However, the merge operation remains successful.

Workaround: None. The correct status is displayed when you perform additional CFS operations.

- CSCeg01551

Symptom: If you issue a **dpvm commit** command, the DPVM application implicitly activates the existing configuration database. The configuration database is activated only when the **dpvm commit** command is explicitly issued after the **dpvm activate** command.

Workaround: None.

- CSCeg12383

Symptom: On rare occasions, the PortChannels with FCIP interface members fail to come up when the switch reboots. This happens when the startup configuration has a default switchport trunk mode setting that does not match the configured trunk mode for PortChannel members (FCIP interfaces). Also, the startup configuration shows any explicit switchport trunk mode setting for the PortChannel.

Workaround: Reconfigure the switchport trunk mode on the PortChannel.

- CSCeg24199

Symptom: Your connection to the server might terminate during an upgrade/downgrade process if the client is detecting the server's status upon receiving events. If the client does not receive any events from the server for a certain amount of time, it assumes that the server is down and closes the connection. Fabric Manager timeouts have also been seen that do not coincide with upgrade/downgrade events.

Workaround: Remove the fabric and then reopen it.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCeg35694

Symptom: If you delete a fabric and then enable the LoadFromDB option while the fabric rediscovers it, there might be a delay in seeing the fabric in the Fabric Manager client.

Workaround: Do not enable the LoadFromDB option in the Fabric Open dialog box when rediscovering the fabric again.
- CSCeg37200

Symptom: Fabric Manager end-to-end connectivity tab does not display properly. The screen turns gray and a java.lang.nullPointerException can be found in the log.

Workaround: Close the dialog and relaunch it.
- CSCeg37598

Symptom: The iSNS server might crash when iSCSI is disabled and iSNS is enabled using Fabric Manager.

Workaround: None.
- CSCeg40856

Symptom: In Fabric Manager, a null pointer exception error message might result in a zone merge recovery on an already recovered fabric.

Workaround: Close the dialog box and relaunch it.
- CSCeg56197

Symptom: Configuring the CIM server certificate as listed below might cause your switch to crash.

 - a. Create a self-certified key (xxxxxx.pem file) on an external server (we use a utility under Hi-Command).
 - b. Enter **conf t** to enter configuration mode.
 - c. Enter **cimserver certificate xxxxxx.pem** to install a certificate specified in the file named with a .pem extension.
 - d. Enter **cimserver enablehttps** to enable HTTPS (secure protocol).
 - e. Enter **cimserver enable** to enable the CIM server.
 - f. Enter **Ctrl-z** to quit

Workaround: None
- CSCeg61535

Symptom: The Telnet server may not be disabled even if you disable it through setup. A telnet session will still work in the switch.

Workaround: Issue the **no telnet server enable** command in configuration mode to disable telnet after you login to the switch.
- CSCeg85146

Symptom: The **show running** command shows the callhome profile alertgroups with an underscore (`_`) rather than a dash (`-`). If the **show running** command in Cisco MDS SAN-OS Release 1.3.x shows callhome profile with alertgroups as an underscore (`_`), then it will carry it over to the release 2.x code and cannot be deleted. This occurs if the following alert groups have been configured:

 - cisco_tac
 - supervisor_hardware
 - linecard_hardware

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: Before upgrading to Cisco MDS SAN-OS Release 2.x, issue the **show running** command and delete the following alert groups:

- cisco_tac
 - supervisor_hardware
 - linecard_hardware
- CSCeh21199

Symptom: If the NetApp file server appliance is configured as an initiator performing a Network Data Management Protocol (NDMP) backup, then the fabric login (FLOGI) process on the MDS switch might terminate because of excessive LSTS requests.

This might happen if your N port or NL port uses extended link services to manage and control a public remote loop. The NetApp file server appliance configuration uses these services, namely LSTS and LINIT, which are documented in the Fibre Channel standards compliance (FC-FLA standard) specification.

Workaround: Upgrade to Cisco MDS SAN-OS Release 2.0(4).

- CSCeh41099

Symptom: Protocol and port numbers, if specified in a IP ACL assigned to a IPSec profile (crypto map), will be ignored.

The interop between Microsoft's iSCSI initiator with IPSec encryption with Cisco MDS 9000 Series switches. If IPSec is configured in the Microsoft iSCSI initiator (also the IPSec/IKE initiator), the host IPSec implementation sends the following IPSec policy:

```
source IP - Host IP, dest IP - MDS IP,
source port - any, dest port - 3260 (iSCSI), protocol - 6 (TCP).
```

Upon receiving the above policy, the protocol and port numbers are ignored and only the IP addresses for the IPSec policy are used. Thus, although iSCSI traffic is encrypted, non-iSCSI traffic (such as ICMP ping) sent by the Microsoft Host in cleartext will be dropped in the MDS port.

Workaround: None.

- CSCeh51924

Symptom: A corrupted entry is created in the snmpTargetParamsTable when a user creates an entry with NULL string in object snmpTargetParamsName as its index. The SNMP service may stop and restart.

Workaround: None. To avoid similar problems, enter a name in snmpTargetParamsName with at least one character when creating a snmpTargetParamsEntry.

- CSCeg66225

Symptom: Password recovery might fail if you use the **copy <config-url> startup** command to save the switch configuration, or if you boot a system image that is older than the image you used to store the configuration and did not use the install all command. The following message might display in syslog or on the console during the process of password recovery.

```
<<%ASCII-CFG-2-ACFG_CONFIGURATION_APPLY_ERROR>>
```

Workaround: Issue the write erase command from the switchboot prompt.



Note

Using the **write erase** command will erase the configuration. You must reapply the configuration, if externally stored, after the switch login.

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

- CSCeg81089

Symptom: A Windows host running Hummingbird 10 with Connectivity Secure Shell 9, cannot use SSH to connect to an MDS switch running Cisco MDS SAN-OS Releases 2.0(x) using the same host configuration as was used when connecting to an MDS switch running 1.3(x) code. The host will display the error, "Authentication Failed, no more shared authentication methods".

Workaround: Reconfigure the client to use "keyboard-interactive" instead of "password" for authentication. To do this, go to tunnel profile settings, select Security Settings>Authentication. Ensure the "keyboard interactive" is the method used, "password" might be the currently configured method. Or upgrade to Cisco MDS SAN-OS Release 2.1(1a).
- CSCeh52280

Symptom: A corrupted license file installs on an MDS 9000 switch without errors.

Workaround: None.
- CSCeh56143

Symptom: A Fabric Manager zone migration wizard causes a Telnet session to hang when a non-MDS switch is present.

Workaround: None.
- CSCeh64080

Symptom: Following an upgrade from Release 1.1 to Release 1.3 or higher, with persistent FC ID enabled, the FC IDs for the storage arrays may get changed after a link flap.

Workaround: None.
- CSCeh65824

Symptom: If you install an SSM and boot it with either the VSFN or SSI Image, the Enterprise License grace period starts.

Workaround: None.
- CSCeg66225

Symptom: Password recovery might fail if you use the **copy <config-url> startup** command to save the switch configuration, or if you boot a system image that is older than the image you used to store the configuration and did not use the install all command. The following message might display in syslog or on the console during the process of password recovery.

```
<<%ASCII-CFG-2-ACFG_CONFIGURATION_APPLY_ERROR>>
```

Workaround: Issue the write erase command from the switchboot prompt.



Note Using the **write erase** command will erase the configuration. You must reapply the configuration, if externally stored, after the switch login.

- CSCei29086

Symptom: Following the installation of a third-party syslog server to a PC running Fabric Manager and Device Manager, the third-party syslog server takes ownership of the PC's IP address as the syslog server. As a result, the MDS switch is no longer able to act as the syslog server.

You can see the error message "java.lang.NullPointerException" if you verify syslog on the MDS switch through Device Manager by choosing **Logs > Syslog > Verify**.

If you uninstall the third-party software and verify syslog again with **Logs > Syslog > Verify**, you see the error message "Can't connect to FM server."

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: To allow the MDS 9000 switch to be the syslog server, follow these steps:

1. Stop or uninstall the third-party syslog server.
 2. Stop Fabric Manager and Fabric Manager Web Services through Windows by right-clicking **My Computer > Manage > Services and Applications > Services**.
 3. Restart Fabric Manager.
- CSCei57342

Symptom: If a link is isolated because of a fabric-binding database mismatch, a reactivation of the corrected fabric-binding database may not initialize the ports.

Workaround: Use the **shut** command followed by the **no shut** command to manually disable then enable the link.

- CSCei58652

Symptom: When a reconfigure fabric (RCF) frames occurs on a VSAN, the ports may be left in a state where the fabric binding is incorrect.

Workaround: None.

- CSCei67982

Symptom: During an upgrade of an MDS switch with two or more MPS-14/2 modules, FCIP tunnels on multiple MPS-14/2 modules can be down at the same time. If a PortChannel of two FCIP tunnels on different MPS-14/2 modules is used for redundancy, the redundancy can be lost. If IVR is running over these FCIP tunnels, IVR can lose remote devices as a result of loss of access over the FCIP based PortChannel.

Workaround: Place other modules on which you can perform a hitless upgrade between the MPS-14/2 modules to allow for more time between module upgrade and to give the FCIP tunnels more time to stabilize. To recover access over the FCIP based PortChannel, reactivate the IVR zone set by adding a dummy zone with two dummy members.

- CSCei91676

Symptom: If iSCSI virtual targets are configured with more than 50 LUN maps, then erroneous overlapping LUN map system messages appear when the iSCSI initiator is not allowed to log in to these iSCSI virtual targets.

Workaround: Limit the number of configured LUN maps for an iSCSI virtual target to fewer than 50 LUNs.

- CSCei91968

Symptom: In a fabric with more than one switch, there is a possibility of CFS or syslog crashing because of a PSS-FULL condition. This happens because of leakage in the PSS records stored by the CFS module.

CFS internal distributions cause a PSS leakage during one of the following:

- An application registration/de-registration. (This is at the rate of 1 PSS records or 60 bytes per event.)
- -An ISL Link flap. (This is at the rate of 2 PSS records per CFS registered application. For 10 CFS registered applications, a 1000 flaps would cause a leak of about 1M.)

Application and Regular CFS distributions in a stable fabric do not result in PSS leakages.

Workaround: None. A switchover will help in cleaning up these records but the usage of the partition remains same (dev/shm partition). However, CFS will reuse the freed space for further PSS storage.

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

- CSCin81851

Symptom: A system switchover causes the boot variables to disappear from display in both the **show running** and **show startup** command outputs. However, the functionality is unaffected, and the boot variables are still set as displayed in the **show boot** command output.

Workaround: Issue the **show boot** command to verify the boot variables.
- CSCeh82490

Symptom: An MDS 9000 switch running SAN-OS 2.0(1b) can potentially send excessive Call Home messages due to a malfunctioning line card that acts as if it were being inserted and removed repeatedly.

Workaround: None.
- CSCeh83514

Symptom: After upgrading to Release 2.0, it is no longer possible to create, modify, or delete the admin role.

Workaround: Before upgrading to Release 2.0, create the admin role.
- CSCeh87985

Symptom: When no role is associated with a user, SNMP fails when the **no role name admin** command is issued to delete the admin role. The SNMP user (admin) has no roles assigned, which causes the failure when there is an attempt to delete a specific role.

Workaround: Associate at least one role (group) to the user by executing the **snmp-server user username [group-name]** command in config mode.
- CSCsc09732

Symptom: If there is a port software failure at the same time as a configuration change for an FCIP interface, the configuration change can fail and subsequent configuration and **show** commands will fail for that FCIP interface.

Workaround: None.
- CSCsc31424

Symptom: Issuing the **no shutdown** command on a port produces this error:

```
fc1/1: (error) port channel config in progress - config not allowed
```

You can reproduce the problem by removing a port from a port channel and then perform a system switchover. However, the problem does not always occur with these steps.

Workaround: Use the **channel-group X** command where port channel X, to configure a new port channel and add the port to it. Then use the **no interface port-channel X** command to remove the newly created port channel. The **no shutdown** command will now be accepted on the port.
- CSCsc33788

Symptom: In rare circumstances, after you issue the **install all** command to upgrade an MDS switch, the upgrade may fail because the installer process fails. When this occurs, you may see a message like the following:

```
%CALLHOME-2-EVENT: SW_CRASH alert for service: installer
The installer failed to respond for 10 times. Exiting ...
Unable to send exit to installer. Return code -1
```

Send documentation comments to mdsfeedback-doc@cisco.com

If you upgrade from 1.3(x) to 2.1 or from 2.0(x) to 2.1 and the upgrade fails, and if after the upgrade failure the supervisor modules are running the new software version, but some modules are running the older software version, then the next attempt to execute the **install all** command will trigger this problem.

You should not encounter this problem if you upgrade from 2.1 to a higher version.

Workaround: There are two ways to address this issue:

- To non-disruptively upgrade all modules that are running the older software version, issue the **install module *module-number* image** command.
 - To disruptively upgrade the modules, issue the **reload module *module-number* force-dnld** command, or reinstall the module.
- CSCsd83775

Symptom: A Fibre Channel Inter-Switch Link (ISL) does not come up and it displays a fabric binding database mismatch error when fabric binding is activated. This problem may be seen when a supervisor switchover occurs or is performed and this ISL comes up. The fabric binding merge activity detects an incompatible database and fails to bring up the link because an incorrect domain ID is being used by the fabric binding module. The fabric binding module on the switch where the switchover occurs would have cleared its local domain ID and be using a domain ID of zero.

Workaround: Issue the **fcdomain restart vsan *vsan-id*** command in the VSANs of interest..

- CSCse99087

Symptom: A user called snmp-user can successfully log into an MDS switch through the CLI, but cannot log in through Fabric Manager or Device Manager. The login attempt fails with this error:

```
SNMP: Unknown username
```

Workaround: None.

- CSCsf21970

Symptom: If you issue immediate, back-to-back commands to delete and then create FCIP interfaces, the internal port service might crash.

Workaround: Wait 5 seconds between the delete and the following create command for a given FCIP interface.

- CSCsg03171

Symptom: The dynamic port VSAN membership (DPVM) failed after the number of F ports exceeded 64 and a port flap occurred.

Workaround: Keep the number of F ports in a switch below 64.

- CSCsg15392

Symptom: If a Generation 1 module has any port that is administratively up, but operationally down when you upgrade from SAN-OS Release 2.x to either Release 3.0(1) or Release 3.0(2x), you might experience traffic disruption on that module.

Workaround: Use the **shutdown** command to shut all the ports operationally down and administratively up on all the Generation 1 modules before upgrading from SAN-OS Release 2.x to Release SAN-OS 3.0(x) or Release 3.0(2x). After the upgrade is complete, the ports can be brought to an administratively up state using the **no shutdown** command.

- CSCeh42252

Symptom: If you try to configure SSH key for any of the non-local user-accounts, in some rare cases you might see a core dump on standby.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: First delete the non-local user-account and create it again so that it becomes a local user-account. Then perform any type of configuration for that user-account. User should not perform configuration operations on non- local user-accounts. Non-local user-accounts can be created due to users getting authenticated using RADIUS/TACACS+ server.

Related Documentation

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

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family 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 VERITAS Storage Foundation for Networks Software*
- *Cisco MDS SAN-OS Compatibility Matrix for SSI Images*
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9000 Family Software Upgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric and Device Manager Online Help*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: <http://support.veritas.com/>

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/>

Send documentation comments to mdsfeedback-doc@cisco.com

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Send documentation comments to mdsfeedback-doc@cisco.com

Documentation Feedback

You can send comments about technical documentation to mdsfeedback-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

Send documentation comments to mdsfeedback-doc@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Send documentation comments to mdsfeedback-doc@cisco.com

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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