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

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.1(2)

Release Date: July 26, 2005

Text Part Number: OL-7411-03 R0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 35.

Note

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	7/25/2005	Created release notes
B0	08/05/2005	Added DDTS CSCeh41099
C0	08/08/2005	Changed the state of DDTS CSCin95832
D0	08/11/2005	Added DDTS CSCeh70232
E0	08/22/2005	Removed DDTS CSCeh61610
F0	08/23/2005	Added DDTS CSCeh61610
G0	11/03/2005	Added DDTS CSCeh69186
H0	12/07/2005	Added DDTS CSCsc31424
I0	12/30/2005	Added DDTS CSCei91968
I1	02/22/2006	Added DDTS CSCsc23435 and CSCsc57865

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

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

J0	05/26/2006	Added DDTS CSCeg33121, CSCeg53114, CSCeg82721, CSCeh30951, CSCeh52973, CSCeh65824, CSCei36082, CSCei55208, CSCei79457, CSCei57342, CSCei58652, CSCei67982, CSCei71686, CSCei86399, CSCei91676, CSCsb89732, CSCsc09732, CSCsc23435, CSCsc28722, CSCsc33788, CSCsc48919, CSCsc57865, CSCsc93936, CSCsc97070, CSCsd07246, CSCsd29338, CSCsd30165, CSCsd71701, CSCsd72822, CSCsd76429, CSCsd89872, and CSCsd94718
K0	06/06/2006	Removed DDTS CSCed16845
L0	08/07/2006	Removed DDTS CSCeg33121, CSCeg84871, CSCeh30951, CSCei10774, CSCei55341 Added DDTS CSCse84811, Revised DDTS CSCsd89872 description Revised status for DDTS CSCei10774, CSCeg90336, CSCeh93109
M0	09/05/2006	Added DDTS CSCsd78967
N0	09/13/2006	Added DDTS CSCsf21970
O0	11/07/2006	Added DDTS CSCse70275, and CSCsg15392
P0	02/23/2007	Added DDTS CSCse99087, CSCsg03171, and CSCsh27840.
Q0	04/04/2007	Added the section "Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch".
R0	08/24/2007	Added DDTS CSCsd83775.

Contents

- , page 3
- System Requirements, page 3

Image Upgrade, page 6

New Features in Cisco MDS SAN-OS Release 2.1(2), page 7

Limitations and Restrictions, page 9

Caveats, page 9

Related Documentation, page 35

Obtaining Documentation, page 36

Documentation Feedback, page 37

Cisco Product Security Overview, page 38

Obtaining Technical Assistance, page 39

-

Introduction

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

-
-

Components Supported

Note

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product

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

	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

	9		
	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-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only

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

Determining the Software Version

Note

show version

Image Upgrade

You can nondisruptively upgrade to Cisco MDS SAN-OS Release 2.1(2) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of the SAN-OS, upgrade to Release 1.3(x) and then Release 2.1(2).

When downgrading from Cisco MDS SAN-OS Release 2.1(2) to Release 1.3(x), you might need to disable new features in Release 2.1(2) for a nondisruptive downgrade. Issuing the 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
```

no device-alias distribute
show incompatibility system bootflash:1.3(x)_filename

Configuration Guide

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

-
-
-

New Features in Cisco MDS SAN-OS Release 2.1(2)

Family Fabric Manager Configuration Guide

Note

Nondisruptive Storage Services Module (SSM) Image Upgrade

Storage Service Modules (SSMs) initially come up in Fibre Channel switching mode by default.

Persistent FC IDs and Domains for IVR

Note

SCSI Flow Services Support for Interfaces

Special Characters in TACACS+ Global Secret Keys

Two special characters are allowed in TACACS+ global secret keys. You can use the dollar sign ($) and the percent sign (%) in TACACS+ global secret keys.

Control for SNMP Notifications for linkUp/linkDown Traps

NASB Storage Array Controller Support

NASB Target Rediscovery

iSCSI Duplicate WWN Check

Fabric Manager Enhancements

-
  -

–
–
–
–

Limitations and Restrictions

SANTap

iSCSI

VSFN Compatibility

Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software

Caveats

Table 3 Open Caveats and Resolved Caveats Reference

	Software Release (Open or Resolved)	
DDTS Number	**2.1(1a)**	**2.1(2)**
Severity 1		

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)

Resolved Caveats

•

copy running-config startup

Workaround

Symptom

Workaround

Symptom

Workaround **Admin > Fabrics**

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround
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.

CSCeh29872

Symptom: The ICMP Path-MTU discovery might not work with IPsec depending upon the SPD policy that is created and where the ICMP error message is originated.

Workaround: Identify the path MTU and set it as the local interface MTU in the switch.

CSCeh39705

Symptom: iSCSI immediate and unsolicited data is not allowed to be used when the data digest is turned on.

Workaround: None.

CSCeh41378

Symptom: If an MDS switch has more than one module that supports Ethernet ports, the Cisco Discovery Protocol (CDP) learns entries over both the Gigabit Ethernet ports and the mgmt0 port. Subsequently, if there is either a system switchover or a restart of the CDP process, CDP will lose neighbors learned over the Gigabit Ethernet ports. A side effect of this behavior is that the **sh cdp neighbors interface *<gig intf>***

gigabitethernet x/y

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

shut

no shut

Symptom

```
%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)
```

module-number

module-number

slot ***slot***

: An IVR zoneset activation fails at any IVR enabled switch and remains in "ready to advertise" state. This happens in very rare cases when the force option is not used while activating the IVR zoneset.

: Deactivate IVR zoneset from an IVR enabled switch where the IVR Zoneset activation status is either "ready to advertise" or "advertising". Note that this step would disrupt IVR traffic. When the deactivation is successful then reactivate the IVR zoneset with the force option.

CSCei52477

: During a single CLI session, if a user repeatedly (over 6000+ times) enters a nested submode and exits all submodes using the command, the system will crash.

: Log out of the session and log in again before continuing operations.

CSCei55208

: In some rare cases, an IVR process may restart if VSANs with IVR devices are continuously suspended and unsuspended while IVR zone set activation is in progress.

: Avoid suspending and unsuspending VSANs with IVR members while IVR zone set activation is in progress.

CSCin93539

: Following the merge of two fabrics, the Fabric Manager Client cannot open.

: Close all fabrics and reopen the new fabric.

CSCin95832

: An installation of the Device Manager following the installation of the Fabric Manager failed the install process was trying to detect the port that will be used by the database server. If the port is taken, the installation displays an error and then quits.By default, the database tries to bind to port 9001. If the port is taken by another application, the database cannot be started.

: Do not check the database server port during installation. If the port is not available and the database server cannot be started, the database updating dialog box hangs. If that occurs, follow these steps to resolve the problem.

1.

2.

3.

-

-

-

- **copy <*config-url***

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

: Issue the write erase command from the switchboot prompt.

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

CSCeg72539

: iSNS server functionality may not restore iSCSI initiator node detail properly after a system switchover. Under this circumstance, iSNS server will not respond correctly to DevGetNext request from an iSNS client. This problem does not happen consistently.

: None

CSCeg84853

: If two fabrics merge, one with automatic VSAN topology and the other configured VSAN topology, and if the autonomous fabric ID assignment as per the user configured topology is not the same as the autonomous fabric ID assignment in the autonomous fabric ID table then sometimes the IVR zone set activation keeps waiting for the switch with the lowest WWW to modify the AFID table to correct the misconfiguration.

Issue the command to clear the IVR session and reactivate the IVR zone set followed by the command.

CSCeh08307

: The Fabric Manager server does not filter VSANs by each client's VSAN scope.

: None.

CSCeh19639

: 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.

: None

CSCeh31983

: The command accepts // - /, even though an image should not be stored on modflash://slot-0/. If it is, the image disappears upon SSM reload.

: Store an SSI image on the SSM flash on modflash://slot-1/ (where is the slot number where SSM is installed) and have the SSI boot variable point to modflash://slot-1/.

CSCeh33814

: The RMON_ALERT e-mail does not send the variable or any information about what alarm is triggered.

: None.

CSCeh33448

: The command does not support the use of modflash:.

: Copy the image back to the supervisor to execute the command.

CSCeh33814

: The RMON_ALERT e-mail does not send the variable or any information about what alarm is triggered.

: None.

CSCeh34275

: iSCSI initiators do not advertise their iqn names on Interop VSAN Fibre Channel name server (FCNS). Fabric Manager will not display them.

: None.

CSCeh35859

: After a process restart or merging with several fabrics simultaneously, the IVR zoneset activation process might hang in the "ready to advertise" state.

: Clear the IVR session by issuing the command and then reactivate the IVR zoneset by issuing the **ivr zoneset activate** *name* < *name*>

zoneset_name *vsan*
zoneset_name

Workaround: Issue **ivr zoneset activate name** *name* **force**
ivr commit

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom
Workaround

Symptom

Workaround

Symptom

Workaround **shutdown/no shutdown**

Symptom
show running-config
show user-account

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom **no role name admin**

Workaround **snmp-server user** *username* [ ] command in config mode.

CSCeh92843

: When an iSCSI host sends a read command to a target and some Fibre Channel data-in frames are not received by an IPS line card but the MDS switch receives a good SCSI status frame from the target, the IPS port can send an iSCSI status PDU with a wrong Status Sequence Number (StatSN) to the iSCSI host, causing it to reset the TCP connection. This scenario has been observed in some rare instances of Fibre Channel cable cut testing.

: None.

CSCei08541

: If there are two FCIP members in the PortChannel, while the traffic is running (at a 1-Gbps rate or any other large rate) bring up the second FCIP link (previously just one FCIP member is up), and you will see the total PortChannel throughput drop to about 10% of the previous number, and this low rate will last for about 25 seconds. This may cause array replication software to timeout on commands and lose sync.

: None.

CSCei17687

: FLOGI service may fail after a switchover due to high availability inconsistency caused when a VSAN, enabled with FICON, is deleted and recreated. The VSAN configuration events should occur before the switchover. The process of bringing up the F port after the switchover triggers the FLOGI service termination. This scenario is very rare and is caused by some race conditions within the FLOGI service.

: None.

CSCei18425

: Fabric Manager does not display FCIP tunnels properly.

: None.

CSCei22596

: When a special frame is enabled for FCIP and FCIP is bound to an Ethernet channel, the IPS port may fail.

: Disable the special frame in FCIP.

CSCei29086

: 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, FM/DM 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."

: To allow FM/DM to be the syslog server, follow these steps:

Stop or uninstall the third-party syslog server.

Stop Fabric Manager and Fabric Manager Web Services thought Windows by right-clicking **My Computer > Manage > Services and Applications > Services**

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom:

show nodes local

Workaround:

Open Caveats

- **Symptom**

  Workaround

- **Symptom**

  Workaround

- **Symptom**

  Workaround

- **Symptom**

  Workaround

  -
  -
  -

Note

- **Symptom**

  Workaround

- **Symptom**

  Workaround

  commit

- **Symptom**

Workaround

```
switch(config)# rscn restrict swrscn-event vsan 1

               no rscn restrict swrscn-event vsan 1
```

no qos enable

Workaround

Symptom

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

vsan-id

```
SCSI CHECK CONDITION     Sense - 0x03 and ASC/ASCQ = 0x3b/0x00
```

```
2005 Sep 15 17:36:55 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:36:56 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:36:59 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:37:43 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:37:44 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:37:47 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:38:31 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:38:32 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:38:35 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
```

suppressed; otherwise, hosts that are registered for RSCN will stop receiving RSCNs.

To use the hidden configuration command to suppress the RSCNs, follow these steps:

Issue the command to identify the port registered for RSCN.

Issue the command to identify the FC interface of port 3.

In configuration mode, use the command to suppress all required interfaces.

4.

5.

6.

- **channel-group X**
  no interface port-channel X
  no shutdown

- **Symptom** **install all**

  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**

  Workaround

  install module **image**
  reload module **force-dnld**

  Symptom

  Workaround

  no system health module *ssm-module-number* **loopback failure-action**

```
copy running-config volatile:
copy volatile: tftp:
```

```
kernel uptime is 137 days 3 hours 49 minute(s) 32 second(s)
 Last reset at -447213060 usecs after Sun Mar 18 05:59:15 2018
   Reason: Not defined
   System version:    Service: §"H
```

```
no ssm enable feature scsi-flow force module
```

```
install all system bootflash:m9500-sf1ek9-mz.2.1.2d.bin kickstart
bootflash:m9500-sf1ek9-kickstart-mz.2.1.2d.bin ssi
bootflash:m9000-ek9-ssi-mz.2.1.2j.bin
```

```
switch(config)# ssm enable feature scsi-flow module
```

```
show module
```

reload module

Last membership update failed: port-channel: required service is not responding
(err_id 0x402B No port

```
SNMP: Unknown username
```

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 Storage Service Interface Images

Cisco MDS 9000 Family SSM Configuration Note

Cisco MDS 9000 Family ASM Configuration Note

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 9020 Fabric Switch Hardware Installation Guide
  Cisco MDS 9000 Family Software Upgrade and Downgrade Guide
  Cisco MDS 9000 Family Configuration Guide
  Cisco MDS 9000 Family Command Reference
  Cisco MDS 9020 Fabric Switch Configuration Guide and 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 Quick Configuration Guide
  Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide
  Cisco MDS 9000 Family MIB Quick Reference
  Cisco MDS 9020 Fabric Switch MIB Quick Reference
  Cisco MDS 9000 Family CIM Programming Reference
  Cisco MDS 9000 Family System Messages Reference
  Cisco MDS 9020 Fabric Switch 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/

Obtaining Documentation

Cisco.com

Product Documentation DVD

Ordering Documentation

-
-
-

Documentation Feedback

You can send comments about Cisco documentation to bug-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

-
-
-

Reporting Security Problems in Cisco Products

-
-
-
-

Tip

Obtaining Technical Assistance

Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

Note

Tools & Resources

Cisco Product Identification Tool **Cisco Product Identification Tool**

show

Submitting a Service Request

Definitions of Service Request Severity

Obtaining Additional Publications and Information

-
- *Internet Protocol Journal*
-
-
-

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2004 - 2005 Cisco Systems, Inc. All rights reserved.