Installation and Configuration for Common Criteria EAL3 Evaluated Cisco MDS 9000 Family – NX-OS Release 4.1(3a)

Version 1.0
August 2009

This document describes how to install and configure Cisco MDS 9000 Family Switches in accordance with the Common Criteria Evaluation Assurance Level 3 (EAL3) evaluated Cisco MDS 9000 Family NX-OS Release 4.1(3a).

Note Any changes to the information provided in this document will result in the Cisco MDS 9000 Family Switch not being compliant with NX-OS Release 4.1(3a) as evaluated and may make it insecure. If the standard MDS documentation conflicts with the guidance in this Installation and Configuration for Common Criteria EAL3 Evaluated Cisco MDS 9000 Family, this guide takes precedence.

Table of Contents

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

List of Tables

List of Figures

Acronyms and Abbreviations

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AES	Advanced Encryption Standard
BIOS	Basic Input/Output System
CCO	Cisco Connection Online
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
DH-CHAP	Diffie Hellmann – Challenge Handshake Authentication Protocol
DSA	Digital Signature Algorithm
FAIS	Fabric Application Interface Standard
FM	Fabric Manager
FC ID	Fiber Channel Identifier
FCIP	Fibre Channel over IP
FC-SP	Fibre Channel – Security Protocol
FICON	Fiber Connection
FM	FM Fabric Manager
GNU	GNU's Not Unix

GUI	Graphical User Interface
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
I&A	Identification and Authentication
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IP-ACL	Internet Protocol – Access Control List
IPFC	IP over Fibre Channel
IPSec	Internet Protocol Security
IQN	iSCSI Qualified Name
ISAPI	Intelligent Storage Application Programming Interface
iSCSI	Small Computer System Interface over IP
ISS	Intelligent Storage Service
JSP	JavaServer Page
LAN	Local Area Network
LUN	Logical Unit Number
MDS	Multilayer Director Switch
NASB	Network-Accelerated Serverless Backup
NTP	Network Time Protocol
nWWN	node World Wide Name
NX-OS	Nexus Operating System
PostgreSQL	Post-Ingres Structured Query Language
pWWN	port World Wide Name
RSA	Rivest, Shamir, Adleman
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSM	Security Services Module
ST	Security Target
sw	switch
sWWN	switch World Wide Name
SYSLOG	SYStem LOG
TAC	Technical Assistance Center

TAC	Terminal Access Controller
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
VSAN	Virtual Storage Area Network
VTY	Virtual TeletYpe
WWN	World Wide Name

Introduction

This document is an addendum to the Cisco MDS 9000 Family NX-OS Release 4.1(3a) documentation set, and should be read before configuring a Cisco MDS 9000 Family Switch in accordance with the Common Criteria Evaluation Assurance Level 3 (EAL3) evaluated NX-OS Release 4.1(3a). This document contains instruction on a variety of security configuration issues and all of the instruction contained within should be followed, unless otherwise stated, when installing or configuring a Cisco MDS 9000 Family Switch in accordance with the Common Criteria evaluated configuration.

Cisco product documentation includes:

- Configuration Guides, which provide a descriptive overview of functions, the commands needed to enable them, and the sequence of operations that should be followed to implement them. The configuration guide should be consulted first when enabling features and functions.
- Command References, which provide a complete and detailed summary of all configuration commands and options, their effects, and examples and guidelines for their use. The command references should be consulted to confirm detailed syntax and functionality options.
- Error Message summaries, which describe all error messages issued by the product.

The following Cisco documentation is referenced by this document:

[1] Cisco MDS 9000 Family Command Reference, Release 4.1(x)

[2] Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x

[3] Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 4.x

[4] Hardware Installation Guides for each Switch platform (see Table 4 in this document)

[5] Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series and Cisco Nexus 2000 Series

[6] Cisco MDS 9000 Family NX-OS Release 4.1(3a) [Security Target]

[7] Cisco MDS 9000 Family System Messages Reference Cisco MDS 9000 NX-OS Release 4.1(1b)

Cisco MDS 9000 Family NX-OS Release 4.1(3a) and the documents listed above can be found on the Internet at:

http://www.cisco.com/

Audience

This document is written for administrators configuring a Cisco MDS 9000 Family NX-OS Release 4.1(3a) Switch in accordance with the Common Criteria evaluated Cisco MDS 9000 Family NX-OS Release 4.1(3a). This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you have been trained in the use of the product and its application. There are no configurable components of the Cisco MDS 9000 Family NX-OS Release 4.1(3a) Switch that are accessible to non-administrative users (end-users), and hence there is no user-level documentation

Supported Hardware and Software Versions

Only the hardware and software version combinations listed in the "ST and TOE Identification" section of the ST **[6]** can be used to implement an evaluated configuration.

Security Information

The sections that follow provide additional security information for use with Common Criteria evaluated Cisco MDS 9000 Family Switches.

Security Implementation Considerations

The sections that follow provide implementation considerations that need to be addressed to administer NX-OS Release 4.1(3a) in a secure manner consistent with Common Criteria evaluated Cisco MDS 9000 Family Switches.

Evaluated Configuration

Only the hardware and software version combinations listed in the "ST and TOE Identification" section of the ST **[6]** can be used to implement an evaluated configuration. Changing the software to a different version invalidates the evaluated status of a particular hardware platform.

The Common Criteria Target of Evaluation (TOE) for Cisco MDS 9000 Family Switches defines only the features identified in the "Toe Summary Specification" section of the ST **[6].** These features are those listed below:

- Security Management (SM)
- Device Access Control (AC)
- Accounting, System Messaging, and Fabric Manager Logs (AL)
- Session Control and Monitoring (CM)
- Encryption Services (ES)
- Identification and Authentication (IA)
- Access Control (ACC)
- Confidentiality (CO)

- Self-Protection of the TOE (SP)

The following hardware and software features and functions of a Cisco MDS 9000 Family Switch are outside the TSF and must NOT be used in the evaluated configuration. Those marked with an asterisk (*) must be disabled by following the guidance in this document. All others are disabled by default and must not be enabled:

- IPFC and In-band Management of the TOE switches
- FCIP
- Switch Command Line Interface (only as accessed through the pull-down menus of the Fabric Manager Client and Device Manager)
- IPSec
- Certificate Authorities and Digital Certificates
- SAN Extension Tuner
- FICON
- Cisco Storage Media Encryption
- Cisco Data Mobility Manager
- Oracle Database
- JBoss jmx-console*
- JBoss web-console*
- Use of Intelligent Storage Services:
  - SCSI Flow Services and Statistics
  - Fibre Channel Write Acceleration
  - SANTap
  - Network-Accelerated Serverless Backup (NASB)
  - Network-Hosted Storage Applications with the Fabric Application Interface Standard (FAIS)-based Intelligent Storage Application Programming Interface (ISAPI). This is an API Cisco provides on the SSM.

NOTE: The Intelligent Storage Services (ISS) capabilities mentioned above are available on the port Fibre Channel Storage Services Module (SSM) but require a separate boot image to be installed on the SSM. This is not allowed in the evaluated configuration.

The evaluated configuration also includes several assumptions and requirements on the TOE environment that must be met by the intended environment in order for the installed TOE to be in the evaluated configuration. These are as follows:

- Network administrators and operators of the TOE are assumed to be non-hostile, trusted to perform their duties in a secure manner, and expected to follow all security policies and procedures applicable to their deployment.
- Internetworking equipment containing the TOE is assumed to be in a physically secure environment.
- Interconnected switches within the same management zone as the TOE are assumed to have protection against unauthorized access.

- Data traversing the VSAN across different environment locations is assumed to be protected from threats of unauthorized disclosure and unauthorized modification.
- It is assumed that administrators, operators and maintainers have been trained sufficiently to configure, operate, and maintain the TOE in a secure and trusted manner in accordance with the guidance documentation.
- Clock sources external to the scope of the TOE are stored in a secure location, and configured accurately so as to provide a trusted clock source for the TOE's internal clock.
- All network devices within the VSAN will be configured to the same external clock.
- The Management LAN is trusted, this means that the TOE is not expected to deal with malicious attacks on its management LAN interface. As such all services such as AAA or NTP provided by the management LAN, and all devices attached to the management LAN are trusted to perform in a secure manner.
- Administrators shall ensure that all users of the TOE use passwords that conform to the complexity requirements as described in the evaluated guidance documentation.

The configuration of the Cisco MDS 9000 Family Switch should be reviewed on a regular basis to ensure that the configuration continues to meet the evaluated configuration particularly in the case of the following occurrences:

- Changes in the Cisco MDS 9000 Family Switch configuration
- Changes in the organisational security policy
- Changes in the threats presented from the untrusted network(s)
- Changes in the administration and operation staff or of the physical environment of the Cisco MDS 9000 Family Switch

NOTE: When specific roles are described in this document the convention from the Security Target is used: role_name (sw or FM). Sw is the abbreviation for switch and FM for Fabric Manager.

Physical Security

The Cisco MDS 9000 Family Switch must be located in a physically secure environment to which only a trusted administrator has access. The secure configuration of a Cisco MDS 9000 Family Switch can be compromised if an intruder gains physical access to the Switch.

Traffic Protection

Ensure that adequate security controls have been deployed to protect against threats of unauthorized disclosure and unauthorized modification of traffic between interconnected entities belonging to the same VSAN (but possibly located in different physical environments).

Monitoring and Maintenance

Cisco MDS 9000 Family Switches provide several ways to monitor their operation, from logs to messages.

- Ensure you know how you will monitor the NX-OS Release 4.1(3a) Switch, both for performance and for possible security issues. See the "Cisco MDS 9000 Family System Messages Reference, Text Part Number: OL-17675-02" sections AAA, ACL, IP ACL, PORT_SECURITY, SECURITYD and ZONE messages.

- Plan your backups. If there should be hardware or software problems, you may need to restore the NX-OS Release 4.1(3a) Switch configuration.

Secure Management

Ensure that management and configuration of the security functions of the TOE are:

a) Initiated from a management station connected to a trusted network
b) Undertaken by trusted staff trained in the secure operation of the TOE
c) Performed securely through the creation of strong passwords in accordance with industry best practices
d) Configured to interface only to trusted clock sources

Securing the IT Environment

The administrator is responsible for ensuring that the IT Environment is configured to adhere with the definition in the Security Target.

NOTE: As the host OS is assumed to be a single-use, stand-alone host, the administrator of the host OS is assumed to be the same as the administrator on the TOE (both a network-admin(sw) and network-admin(FM)).

Specifically, the administrator must:

- Ensure that the host OS on which TOE software is installed is setup to require I&A before allowing access to the host OS.
- Ensure that the host OS on which TOE software is installed is setup to restrict access to the filesystem to the locally authenticated administrator.

Modes of Operation

An MDS 9000 Family Switch has several modes of operation, these modes are as follows:

Booting : While booting, the switches drop all network traffic until the NX-OS image and configuration has loaded. This mode can transition to any of the following modes:

- Loader Prompt/Kickstart Mode: When either of the system images is corrupted and/or unusable.
- Setup: When the NX-OS loads and no configuration has been saved to the switch.
- Normal: When the NX-OS images and configuration are loaded successfully and uninterrupted.

Loader Prompt/Kickstart Mode: While the switch is in this mode, no network traffic is routed between the network interfaces. It should be noted that while no administrator password is required to enter the kickstart or loader mode, physical access to the switch is required, therefore the switch should be stored in physically secure location to avoid unauthorized access which may lead to the switch being placed in an insecure state. This mode allows an administrator logged into the console port to specify a NX-OS image on a TFTP server to load. In this mode the switch does not handle any network traffic, apart from what is required to perform the TFTP boot, thus preventing an insecure state. On reload or power-up of the chassis, the switch attempts to go to system mode and will stop at either loader or kickstart mode due to the following conditions:

1. System will stop at loader mode if there is no Kickstart image configured to be loaded.

2. System will stop at Kickstart mode, if user explicitly boots up only the Kickstart image or if the system image is not compatible or is corrupted.

Once a valid system image is located and loaded the switch is reloaded and enters Normal boot mode.

Setup: The switch enters this mode after booting if no configuration exists (e.g., First boot). In this mode the switch has no IP address and therefore does handle network traffic, thus preventing an insecure state. This prevents the switch from booting into an insecure state. The switch starts an interactive setup program to allow the administrator to enter basic configuration data, such as the switch's IP address, administrator password, and management channels. When the setup program is exited, the switch transitions to the Normal mode.

Normal: The NX-OS image and configuration is loaded and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all TOE security functions are operating. While operating the TOE has little interaction with the administrator. However, the configuration of the TOE can have a detrimental effect on security. Mis-configuration of the TOE could result in the unprotected network having access to the internal/protected network.

If an operational error occurs the switch reboots (once power supply is available) and enters booting mode.

Specific Supervisor Modes

The 9500 series of MDS switches can be deployed with a single or redundant pair of supervisors. The supervisor modules have some additional modes of operation.

Table 1 Specific Supervisor Modes

Active	The active supervisor module in the switch is ready to be configured.
HA standby	A switchover is possible.
Offline	The switch is intentionally shut down for debugging purposes.
Unknown	The switch is in an invalid state and requires a support call to TAC.

Redundancy Modes for Supervisor

Table 2 Redundancy Modes for Supervisor

Not present	The supervisor module is not present or is not plugged into the chassis.
Initializing	The diagnostics have passed and the configuration is being downloaded.
Active	The active supervisor module and the switch is ready to be configured.
Standby	A switchover is possible.
Failed	The switch detects a supervisor module failure on initialization and automatically attempts to power-cycle the module three (3) times. After the third attempt it continues to display a failed state.
Offline	The supervisor module is intentionally shut down for debugging purposes.
At BIOS	The switch has established connection with the supervisor and the supervisor module is performing diagnostics.
Unknown	The switch is in an invalid state. If it persists call TAC.

Internal Redundancy States

Table 3 Internal Redundancy States

HA standby	The HA switchover mechanism in the standby supervisor module is enabled. See the section "HA Switchover Characteristics".
Active with no standby	A switchover is possible.
Active with HA standby	The active supervisor module in the switch is ready to be configured. The standby module is in the HA-standby state.
Shutting down	The switch is being shut down.
HA switchover in progress	The switch is in the process of changing over to the HA switchover mechanism.
Offline	The switch is intentionally shut down for debugging purposes.
HA synchronization in progress	The standby supervisor module is in the process of synchronizing its state with the active supervisor modules.
Standby (failed)	The standby supervisor module is not functioning.
Active with failed standby	The active supervisor module and the second supervisor module is present but is not functioning.
Other	The switch is in a transient state. If it persists call TAC.

Installation Notes

The following documentation should be followed when installing a Cisco MDS 9000 Family evaluated NX-OS Release 4.1(3a) Switch:

Table 4 Installation Documentation for Cisco MDS 9000 Family Hardware Platforms

Hardware Family	Installation Information
Cisco MDS 9100 Series	*Cisco MDS 9100 Series Hardware Installation Guide*
Cisco MDS 9216 Switch	*Cisco MDS 9216 Switch Hardware Installation Guide*
Cisco 9500 Series	*Cisco MDS 9500 Series Hardware Installation Guide*

Verification of Image and Hardware

To verify that the Cisco MDS 9000 Family Switch software and hardware have not been tampered with during delivery, execute the following procedures:

1. Before unpacking the hardware, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).
2. Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

3. Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

4. Verify that the box has indeed been shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. For equipment shipped directly from Cisco, this can be done online through the order status tool: http://www.cisco.com/cgi-bin/status. For other suppliers, this check should be performed by some mechanism that was not involved in the actual equipment delivery, e.g., phone/FAX or other online tracking service.

5. Download a Common Criteria evaluated software image file from Cisco Connection Online (CCO) for your specific hardware platform as per Table 10 onto a trusted computer system. For all images, ensure that you have sufficient system and flash memory to support the image on your Switch hardware by checking the Release Notes appropriate to NX-OS Release 4.1(3a). Software images are available from CCO at the following URL:

   http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=277381371

6. Once the image file(s) have been downloaded, verify that it has not been tampered with by using an MD5 utility to compute a MD5 hash for the downloaded file and comparing this with the MD5 hash for the image listed in this document (Table 5: NX-OS Release 4.1(3a) Images and MD5 hash values). If the MD5 hashes do not match, contact Cisco Technical Support.

7. Install the downloaded and verified software image onto your Cisco MDS 9000 Family Switch as described in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2].**

8. Start your NX-OS Release 4.1(3a) Switch as described in the installation documentation (see Table 4 above). Confirm that your NX-OS Release 4.1(3a) Switch loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console. At the prompt, type the **show version** command (see Figure 1 below). Verify that the version is one of the valid versions listed in the ST **[6].** If the NX-OS Release 4.1(3a) image fails to load, or if the NX-OS Release 4.1(3a) version does not match one of the valid versions listed in the ST **[6],** contact Cisco Technical Support.

Figure 1 Example of "show version" Output, Showing NX-OS Release Version

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html

Software
  BIOS:      version 1.0.10
  loader:    version N/A
  kickstart: version 4.1(3a)
  system:    version 4.1(3a)
  BIOS compile time:       01/08/09
  kickstart image file is: bootflash:/m9500-sf2ek9-kickstart-mz.4.1.3a.bin
  kickstart compile time:  2/12/2009 19:00:00 [03/06/2009 05:35:52]
  system image file is:    bootflash:/m9500-sf2ek9-mz.4.1.3a.bin
  system compile time:     2/12/2009 19:00:00 [03/06/2009 09:02:09]

Hardware
  cisco MDS 9506 (6 Slot) Chassis ("Supervisor/Fabric-2")
  Motorola, 7447A, altivec  with 1032436 kB of memory
  Processor Board ID JAB110701NB

  Device name: MDS9506
  bootflash:    1000440 kB
  slot0:           0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 13 minute(s), 36 second(s)

Last reset
  Reason: Unknown
  System version: 4.1(3a)
  Service:
```

Externally Visible Ports

Below is a listing of protocols and ports that are accessible on the external interfaces facing the remote host when the switch and Fabric Manager are in its Common Criteria evaluated configuration.

Switch and Fabric Manager IP protocols:

PROTOCOL	SERVICE
1	icmp
6	tcp
17	udp

Table 5 Switch Open Ports

IP Protocol	Port	Named Service	Description
TCP	22	ssh	Sshv2 used by Fabric Manager and Device Manager
	80	http	Web server used to download Device Manager
UDP	161	Snmp	Snmpv3 used by Fabric Manager and Device Manager

Table 6 Fabric Manager Open Ports

IP Protocol	Port	Named Service	Description
TCP	443	https	jBoss Web Server, used by the Fabric Manager Web Client when HTTPS is enforced (by following the administrative guidance) 443 is used rather than 8080
	4444	N/A	used by jBoss Web Server, used to accept remote calls from Fabric Manager Client
	5001	N/A	web service used for communication between the Fabric Manager and the Device Manager
	8009	N/A	Apache JSP , integrates TomCat into jBoss web server and allows it to use the server's SSL processing. Listens on 8009 and redirected to 8443, a non-external listening port.
UDP	None		

Configuration Notes

The Common Criteria Target of Evaluation (TOE) for Cisco MDS 9000 Family NX-OS Release 4.1(3a) defines the following security features.

- Security Management
- Device Access Control
- Accounting Log
- Session Control and Monitoring
- Encryption Services
- Identification and Authentication
- Access Control
- Confidentiality
- Self-Protection of the TOE

Upon delivery, a Cisco MDS 9000 Family Switch is not configured to support any of the security functions described above. These functions must be explicitly configured as described in the product documentation and this document to ensure your Cisco MDS 9000 Family Switch is operating in accordance with Common Criteria evaluated Cisco MDS 9000 Family NX-OS Release 4.1(3a) configuration.

Security Features

The configuration information provided in this document should be followed when the particular feature of the TOE is to be configured. Where no evaluation specific guidance has been provided, Security features of the TOE should be configured as described in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* chapters listed below:

Table 7 Evaluated Security Features for Cisco MDS 9000 Family Switches

Feature	Chapter and Section in Configuration Guide [2]
Security Management	Chapter 2 Before you Begin
Default Switch Roles	Chapter 32 Configuring Users and Common Roles Role-Based Authorization
Configuring User Account	Chapter 34 Configuring RADIUS and TACACS+ Switch AAA functionalities
Device Access Control	Chapter 24 Configuring and Managing Zones Zone Configuration Chapter 43 Configuring iSCSI iSCSI Access Control Chapter 40 Configuring Fabric Binding Fabric Binding Configuration Chapter 35 Configuring IPv4 and IPv6 Access Control Lists Chapter 39 Configuring Port Security
Accounting Log	Chapter 52 Configuring System Message Logging
Session Control and Monitoring	Chapter 2 Before you Begin Configuring the Switch Banner Message Displaying Users Setting the Terminal Timeout Chapter 32 Configuring Users and Common Roles Configuring User Account Displaying User Account Information.
Encryption Services	The password encryption functionality is not configurable. Chapter 32 Configuring Users and Common Roles Creating or Updating User Configuring SSH Services
Identification and Authentication	Chapter 5 Initial Configuration Telnet Server Connection Chapter 31 Configuring Users and Common Roles Configuring SSH Services Creating or Updating Users Displaying Use Account Information.

Feature	Chapter and Section in Configuration Guide [2]
	Chapter 34 Configuring RADIUS and TACACS+ Configuring RADUIS Configuring TACACS+ Local AAA Services Switch AAA functionalities Chapter 43 Configuring iSCSI iSCSI Authentication Setup Guidelines and Scenarios
Access Control	Chapter 32 Configuring Users and Common Roles Role-Based Authorization
Confidentiality	Chapter 20 Configuring and Managing VSANs Chapter 22 Creating Dynamic VSANs Chapter 44 Configuring IP Services Overlay VSAN Configuration Multiple VSAN Configuration
Self-Protection of the TOE	The domain separation functionality is not configurable. Chapter 5 Initial Configuration Configuring Date and Time

Security Management

The network administrator should ensure that all user's passwords meet the minimum requirements of the organisations security policy. It is recommended that passwords contain:

- At least 8 characters
- Both upper and lower case characters
- At least 1 special character (`~!@#$%^&*()-_=+)
- At least 1 number (0-9)

It is also recommended that users change their passwords once every 45 days.

To assist in this area, NX-OS will enforce the following password requirements for local, SSH and SNMP password mechanisms:

- At least eight characters long
- Does not contain many consecutive characters exceeding three consecutive characters (e.g., "123" is permitted, but "1234" is not)
- Does not contain many repeating characters exceeding two repeated characters (e.g., "aa" is permitted but "aaa" is not)
- Does not contain dictionary words
- Contains both upper and lower case characters
- Contains numbers

Additionally, although not automatically enforced by the TOE, all other identification and authentication mechanisms participating within the TOE including DH-CHAP, CHAP and Fabric

Manager Web Services remote login passwords must configure a password that meets the above requirements.

During the initial setup the administrator should change the default password.

The network-admin (sw) role can create, modify and delete users and roles to control the way the switch is accessed and operated. The network-admin (sw) role has sole responsibility for the security of the switch through the ability to change the default security values. Users with the network-admin (sw) role can create additional roles.

SEE: "Configuring User and Common Roles" and "Configuring RADIUS and TACACS+" in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 4*.x **[2]** for further information.

Device Access Control

Port Security

Port security allows the network-admin (sw) role to configure the switch to reject login requests from unauthorized Fibre Channel devices (Nx ports) and switches (xE ports). Port security is enforced by the switch by configuring the devices and switch port interfaces through which each device or switch is connected. The port security policy for the TOE must be configured during installation.

The port world wide name (pWWN) or the node world wide name (nWWN) is used to specify the Nx port connection for each device. The switch world wide name (sWWN) is used to specify the xE port connection for each switch. Each Nx and xE port can be configured to restrict a single port or a range of ports.

All the options of the 'port security' command are allowed in the evaluated configuration except for the "any-wwn interface" command. This command would allow an attacker to spoof WWNs and violate policy. The specific policy to be implemented is not dictated by this evaluated configuration. The policy is specific to each customer's environment and should represent the local security policy.

Following activation of port security manually configure the TOE port security policy or enable the auto-learning mode to configure the policy. If you use auto-learning mode, you must disable it after the initial policy is configured.

SEE: "Configuring Port Security" in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Fabric Binding Security

Fabric binding extends port security by binding inter-switch links within the SAN, thus preventing unauthorized switches from joining the fabric or disrupting current fabric operations. Fabric binding policies are enforced based on identities authenticated by DH-CHAP.

All the options of the 'fabric binding' command are allowed in the evaluated configuration. The specific policy to be implemented is not dictated by this evaluated configuration. The policy is specific to each customers environment and should represent the local security policy.

Fabric binding policies are enforced based on identities authenticated by DH-CHAP.

SEE: "Configuring Fabric Binding" in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Zone Security

Zoning enables the network-admin (sw) role to set up access control between storage devices or user groups within the same VSAN. Access to a zone is enforced by examining the source-destination ID field. Zone membership criteria are based on WWNs or FC IDs, including:

- Port, node or switch World Wide Name (WWN)
- IP address
- Fibre Channel Identifier (FC ID)
- Interface and domain ID
- Logical Unit Number (LUN)
- iSCSI qualified name (IQN)
- Symbolic-node-name (IQN)

A zone consists of multiple zone members.

- Members in a zone can access each other; members in different zones cannot access each other.
- If zoning is not activated, all devices are members of the default zone.
- If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.
- Zones can vary in size.
- Devices can belong to more than one zone.
- A physical fabric can have a maximum of 16,000 members. This includes all VSANs in the fabric.

All the options of the 'zone' command are allowed in the evaluated configuration. The specific policy to be implemented is not dictated by this evaluated configuration. The policy is specific to each customers environment and should represent the local security policy.

NOTE: The zone security policy for the TOE must be configured during installation.

NOTE: Hard zoning is enforced by the hardware on each frame sent by an Nx port. As frames enter the switch, source-destination IDs are compared with permitted combinations to allow the frame at wirespeed. Hard zoning is applied to all forms of zoning. Hard zoning enforces zoning restrictions on every frame, and prevents unauthorized access.

SEE: "Configuring Zones" in *Cisco MDS 9000 the Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

LUN Zone Security

Storage devices with multiple Logical Unit Numbers (LUNs) may be zoned separately via LUN Zoning. LUN zoning enables the network-admin (sw) role to restrict access to specific LUNs associated with a device. This type of zoning allows greater access granularity within a storage device.

iSCSI-based access control is applicable only if static iSCSI virtual targets are created. For a static iSCSI target, you can configure a list of iSCSI initiators that are allowed to access the targets. By default, static iSCSI virtual targets are not accessible to any iSCSI host. You must explicitly configure accessibility to allow an iSCSI virtual target to be accessed by all hosts. The initiator access list can contain one or more initiators. The iSCSI initiator can be identified by one of the following mechanisms:

- iSCSI node name

- IPv4 address and subnet
- IPv6 address

All the options of the 'iscsi virtual-target' command are allowed in the evaluated configuration. The specific policy to be implemented is not dictated by this evaluated configuraiton. The policy is specific to each customers environment and should represent the local security policy. This feature is not mandatory in the evaluated configuraiton, it is applicable only if the customers local security policy requires additional control of LUN zoning, beyond standard Zone Security.

SEE: "iSCSI Access Control" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

IP Access Control Lists

In the evaluated configuration, the administrator is required to configure and apply an access control list to permit only SSH, HTTP, SNMP, and ICMP to the switch management port, and to only that access from IP addresses on internal/protected subnets. An example format for such an access list has been provided below. Once the access list has been applied to the mgmt0 interface, the only externally visible ports will be those listed in the "Switch Open Ports" table of this document.

IP-ACLs restrict IP-related MDS 9000 out-of-band (i.e., Ethernet based) management traffic based on IP addresses (Layer 3 and Layer 4 information). An IP-ACL is a sequential collection of permit and deny conditions that apply to IP flows. Each IP packet is tested against the conditions in the list. The first match determines if the software accepts or rejects the rule.

The network-admin (sw) role can specify IP-ACLs using an assigned name. Each IP-ACL can have a maximum of 256 entries. Each entry is a unique filter applied to a specified interface. Each switch can have a maximum of 64 IP-ACLs. Traffic coming into the switch is compared to IP-ACL entries based on the order that the entries occur in the switch. New statements are added to the end of the list. The TOE keeps looking until it has a match. If no matches are found when the switch reaches the end of the list, the traffic is denied. There is an implied deny for traffic that is not permitted. A single-entry IP-ACL with only one deny rule has the effect of denying all traffic.

IP-ACLs are only configurable on the management interface by the network-admin (sw) role.

The **access-list** command operates on a first match basis. Therefore, the last rule added to the access list is the last rule checked. The administrator should make a note of the last rule during initial configuration, because it may impact the remainder of the rule parsing. The NX-OS Release 4.1(3a) default rule is to drop all packets that do not match a rule in the access-list. Therefore if the only rule is a deny rule is put in place this implies that all packets will be dropped.

To enable logging of access-list matches, the log-deny keyword must be used with access-list definitions.

A privileged authorized administrator may manipulate the ACLs using the commands ip access-list and ip **access-group** as described in the *Cisco MDS 9000 Family Command Reference* **[1].** When this policy is applied, the administrator allows traffic from the remote management station using TCP port 22 for SSH, TCP port 80 for HTTP and UDP port 161 for SNMP.

Note that the commands below give example text such as IP addresses, device names, keys, and passwords. For this text noted in italics do not use the given values, but replace them with the relevant information from your network. In this example, the remote administration station is IP address 1.2.3.4 and the TOE management interface is 10.1.1.1.

```
switch(config)# ip access-list restrictmgmt permit tcp 1.2.3.4 0.0.0.0 10.1.1.1
0.0.0.0 eq port 22
switch(config)# ip access-list restrictmgmt permit tcp 1.2.3.4 0.0.0.0 10.1.1.1
0.0.0.0 eq port 80
```

```
switch(config)# ip access-list restrictmgmt permit icmp 1.2.3.4 0.0.0.0 10.1.1.1
0.0.0.0
switch(config)# ip access-list restrictmgmt permit udp 1.2.3.4 0.0.0.0 10.1.1.1
0.0.0.0 eq port 161
switch(config)# ip access-list restrictmgmt deny ip any any log-deny
switch(config)# interface mgmt0
switch(config-if)# ip access-group restrictmgmt in
```

All the options of the 'ip access-list' and 'ip access-group' commands are allowed in the evaluated configuration. In the evaluated configuration, the administrator is required to configure a default access control list policy to protect the switch from any other access other than approved administrative access using ssh, snmp or ICMP.

SEE: "Configuring IP Access Control Lists" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Accounting Logs

The accounting and system message logs on the switch record the start-up and shutdown of the audit functions, all user actions on the switch such as login and logout and all commands executed by the user. Unauthorized access to switch ports and channels on the TOE are also recorded in the accounting log. The TOE records the date and time of each event, the type of event, the involved subject identity and the outcome of the event. The accounting and system message logs are stored for later review and analysis.

Logged messages for these events can be directed to the switch console, local disk or to a syslog server in the IT Environment using the SYSLOG protocol. Only the network-admin(sw) and network-operator(sw) roles can view the accounting and system message logs and review the audit messages stored in the switch buffer on the TOE and act upon them as required.

Note that although the switches can be configured to send log events to a syslog service listening on the Fabric Manager, that this functionality was not evaluated and cannot be enabled in the evaluated configuration.

SEE: "Configuring System Message Logging" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

The network-admin (FM) can view the audit messages stored on the Fabric Manager server by logging into the Fabric Manager Web Client, and navigating to the "Admin, Logs" page. The web server logs can be viewed in the "Fabric Manager (Web)" log, and the Fabric Manager Server logs can be viewed in the "Fabric Manager Server" log.

These logs can also be viewed by users on the host Windows operating system by navigating to the "C:\Program Files\Cisco Systems\MDS 9000\logs" directory and opening either the fm_web.log for the web server logs or fmserver.log for the Fabric Manager Server logs.

Note that on Solaris and Linux systems, the fm_web.log and fmserver.log files are located in /usr/local/cisco_mds9000/logs or $HOME/cisco_mds9000/logs, depending on the permissions of the user doing the installation.

The Cisco *MDS 9000 Family System Messages Reference Cisco MDS 9000 NX-OS Release 4.1(1b)* **[7]** may be of assistance to an administrator in determining the action to be taken in response to the various audit messages that may be logged.

It should be noted that Start-up and shutdown of the audit functions, Login and logout events of users, all commands executed by the user, intrusion attempts on the TOE fibre channel switch ports and AAA events from external RADIUS and TACACS+ servers are considered security relevant events for the TOE. However, other events may also be considered security relevant in a user's installation of the TOE and environment.

Session Control and Monitoring

Session Controls

The network-admin (sw) role can configure the shell session timeout value that specifies the lifetime of all terminal sessions on the TOE. When the time limit is exceeded the shell exits and closes that session. The default is 30 minutes. The network-admin (sw) role can configure different timeout values for a console or a virtual terminal line (VTY) session.

The network-admin (sw) role can also configure the terminal session timeout value that specifies the automatic logout time for the current terminal session on that switch. When the time limit configured by this command is exceeded, the switch closes that session and exits. The default is 30 minutes.

SEE: "Before You Begin" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

User Sessions

The network-admin (sw) and network-admin (FM) role can display a list of all logged in users, and has the ability to terminate a user session. In addition, the network-admin (sw) role can, on the switch, specify an account timeout period upon creation of the user's account, display a user's profile details, and view a user's command history through the accounting log.

SEE: "Configuring Users and Common Roles" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Identification and Authentication

User Types

The TOE maintains user profiles. Authentication information, user name, user password, password expiration date, and role membership are stored in the user profile. The user profile also contains SNMP security parameters that determine the way their SNMP session is established and maintained (e.g., session encryption parameters), a SSH key for secure remote management access to the TOE and an optional expiry date for their account. Only SNMP Version 3 is to be used in accordance with the evaluated configuration.

To enforce SNMPv3 message encryption globally on all the users, use the following command in global configuration mode:

```
switch(config)# snmp-server globalEnforcePriv
```

Individual users must be explicitly allowed access. To do this locally (on the switch), use the following command in global configuration mode:

NOTE: The commands below give example text such as IP addresses, device names, keys, and passwords. For the text noted in italics do not use the given values, but replace them with the relevant information from your network.

```
switch(config)#  snmp-server user testadmin auth sha yyt687E2 priv
aes-128 uDrEw3P01
```

NOTE: Ensure that any accounts defined for the SNMP server use SHA for authentication and AES-128 for privacy**.**

This also enables the AES block cipher for SNMP message encryption (which is stronger than the default, DES). For more guidance on the parameters of this command see "snmp-server user" in *Cisco MDS 9000 Family Command Reference* **[1].**

You must ensure that no SNMP communities are configured, so that SNMPv1 and v2c connections are not allowed.

To view the list of defined communities, use the following command:

```
switch# show snmp community

Community                Group / Access
---------                --------------
```

To delete communities, use the following command in global configuration mode where snmp_Community is the name of the SNMP community:

```
switch(config)#  no snmp-server community snmp_Community
```

Users configured through the CLI are different from users configured through SNMP. These configurations do not directly correspond with each other. However, their passwords may be synchronized for ease of management.

SEE: "Configuring SNMP" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Disabling Telnet

The Telnet service is on by default on the switch. The evaluated configuration requires that the telnet service be disabled. To achieve this use the following command in global configuration mode:

```
switch(config)# no telnet server enable
```

NOTE: Although provided, the Device Manager and Fabric Manager Client's Command Line Interface to the switch is not to be used in the evaluated configuration. In their default setting they are configured to use telnet, which the switch does not allow with the command above in place. This results in them being unusable.

External AAA Service

RADIUS/TACACS+ can also be leveraged for centralized switch and host authentication via the client modules. Both RADIUS and TACACS+ may be used in the evaluated configuration. Any host keys (passwords) that are defined for RADIUS/TACACS+ authentication must comply with the password requirements of this guide.

Note that the commands below give example text such as IP addresses, device names, keys, and passwords. For this text noted in italics do not use the given values, but replace them with the relevant information from your network.

```
switch# config terminal
switch(config)# radius-server host 10.10.0.0 key at9iR7ee
```

and/or

```
switch(config)# tacacs+ enable
switch(config)# tacacs-server host 171.71.58.91 key 0p81kuyy
```

Similar steps can be followed to define a TACACS+ group and apply the group to the aaa authentication command.

```
switch(config)# aaa group server radius radservers
switch(config-radius)# server 1.2.3.4
switch(config-radius)# exit
switch(config)# aaa authentication login default group radservers
switch(config)# aaa authentication login console group radservers
```

SEE: "Configuring RADIUS and TACACS+" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

DH-CHAP Authentication

DH-CHAP is a mandatory password-based, key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication. DH-CHAP authentication in each direction requires a shared secret password between the connected devices. DH-CHAP is not enabled by default, so you must use the following command in global configuration mode to enable it:

NOTE: The commands below give example text such as IP addresses, device names, keys, and passwords. For this text noted in italics do not use the given values, but replace them with the relevant information from your network.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fcsp enable
```

Each switch must have a password configured for DH-CHAP authentication. The 0 in the next command signifies that the password is being entered in clear-text form. If a 7 was substituted for the 0 the command line would read the value after the 7 as the hashed version of the password. The passwords entered as shared secrets must conform to the password complexity guidance outlined in this text.

```
switch(config)# fcsp dhchap password 0 yyt8i9i8
```

or using the previously hashed value of the password and level 7 option:

```
switch(config)# fcsp dhchap password 7 bux8a9d8
```

The destination switch must have a password configured to complete the authentication. The password is specific to the defined device name.

```
switch(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e
password j719ppre
```

The DH-CHAP authentication mode must be changed to "on" for each interface that communicates with other switches, to force DH-CHAP authentication. Use the following command in **interface** configuration mode for each appropriate interface:

```
switch(config)# interface fc1/1
switch(config-if)# fcsp on
```

Repeat these steps on the connecting MDS Switch.

SEE: "Configuring FC-SP and DHCHAP" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

iSCSI (CHAP) Authentication

The IP Storage Services and Multiprotocol Services Modules supports the iSCSI authentication mechanism to authenticate iSCSI hosts that request access to storage. When iSCSI authentication is enabled, the iSCSI hosts must provide user name and password information each time an iSCSI session is established. During an iSCSI login, both the iSCSI initiator and target have the option to authenticate each other. By default, the IPS module allows either CHAP authentication or no authentication from iSCSI hosts. Please note that CHAP authentication is always to be used in accordance with the evaluated configuration. The IPS module verifies the iSCSI host authentication using the local password database, TACACS+, or RADIUS. Use of any of these authentication databases is acceptable in the evaluated configuration.

By default, the IPS module allows either CHAP authentication or no authentication from iSCSI hosts. CHAP authentication is always to be used in accordance with the evaluated configuration. To ensure this, enter the following commands in global configuration mode:

NOTE: The commands below give example text such as IP addresses, device names, keys, and passwords. For this text noted in italics do not use the given values, but replace them with the relevant information from your network.switch# config terminal**.**

Enter configuration commands, one per line. End with CNTL/Z.

switch(config)# **iscsi enable**
switch(config)# **aaa authentication iscsi default local**
switch(config)# **iscsi authentication chap**
switch(config)# **iscsi interface vsan-membership**
switch(config)# **username *icsiuser* password *uut890p0q* iscsi**

The last command must be entered for each iSCSI user. This configures CHAP authentication using the local user database. Authenticating using a AAA service is also possible.

SEE: "Configuring iSCSI" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Encryption Services

Enabling SSH

When using SSH for remote administration the Cisco MDS 9000 Family Switch must be configured to use SSH version 2 and to use DSA or RSA keys with a key size of 1024 or 2048 only. Specification of keys can be performed using the following commands in global configuration mode where keysize is 1024 or 2048:

switch# **config term**
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# **ssh key dsa 1024 force**
switch(config)# **ssh server enable**

When changing keys they will be overwritten. If you wish to change your current key you must add the command 'force' to the end of the commands listed above.

SSHv1 is not to be used in the evaluated configuration. To confirm that SSH version 1 will not be used type the following commands:

```
switch# show ssh server
ssh is enabled
version 2 enabled
```

SEE: "Configuring Users and Common Roles" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Hashed Shared Secret Password

DH-CHAP authentication in each direction requires a shared secret password between the connected devices. This shared secret password is hashed using a negotiated hash algorithm before performing authentication. Supported hash algorithms include MD-5 (first) and SHA-1 (second), though the order in which they are negotiated is configurable by the network-admin (sw) user role. Cisco MDS switches support a default hash algorithm priority list of MD5 followed by SHA-1 for DH-CHAP authentication.

NOTE: RADIUS and TACACS+ protocols always use MD5 for CHAP authentication. Using SHA-1 as the hash algorithm may prevent RADIUS and TACACS+ usage—even if these AAA protocols are enabled for DH-CHAP authentication.

NOTE: Use of DH-CHAP_GROUP_NULL is not permitted in the evaluated configuration because it excludes the Diffie-Hellman key exchange.

Access Control

The TOE has default switch management user roles: network-admin (sw) and network-operator (sw). The network-admin (sw) role has permission to execute all commands and make configuration changes on the switch, including the creation and customization of up to 64 additional roles. The network-operator (sw) role only has permission to view the switch configuration. The network-operator (sw) cannot make any configuration changes to the switch.

The switch roles network-admin (sw) and network-operator (sw) cannot be changed or deleted. However, customized roles can be created to assign to switch users requiring similar privileges to the network-admin(sw) and network-operator(sw) roles.

Additionally, the TOE has default Fabric Manager user roles: network-admin (FM) and network-operator (FM). The network-admin (FM) role has permission make configuration changes on the Fabric Manager, including the addition of FM user roles. The network-operator (FM) role only has permission to view the configuration.

SEE: "Configuring Users and Common Roles" in Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x [2] for further information.

Time Sources

Switches configured in accordance with the Cisco MDS 9000 Family NX-OS Release 4.1(3a) evaluation must timestamp system log messages. All Switches in the Cisco MDS 9000 Family evaluation have internal real time hardware clocks, these clocks provide reliable time stamp for audit logs. Administrators are required to check the system time on a regular basis and adjust it as necessary to maintain accurate time.

The switch may be configured to use a trusted NTP service to ensure the time is kept up to date instead of manually adjusting the time. This can be done using the following commands in global configuration mode:

NOTE: The commands below give example text such as IP addresses, device names, keys, and passwords. For this text noted in italics do not use the given values, but replace them with the relevant information from your network.

```
switch# config term
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 1.2.3.4
```

NOTE: As per the ST **[6]** the NTP Server or NTP Peer must exist within the trusted Management LAN.

SEE: "Initial Configuration" in *Cisco MDS 9000 Family CLI Configuration Guide, Release 4.x* **[2]** for further information.

Saving Configuration

NX-OS uses both a running configuration and a starting configuration. Configuration changes affect the running configuration, in order to save that configuration the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by using the **copy running-config startup-config** command. These commands should be used frequently when making changes to the configuration of the Switch. If the Switch reboots and resumes operation when uncommitted changes have been made, these changes will be lost and the Switch will revert to the last configuration saved.

```
switch# copy running-config startup-config
[########################################] 100%
```

Setting the System Clock

To provide accurate time stamps for logging, the system clock must be set. All MDS 9000 Family Switches have real time clocks that maintain real time when the Switch is powered down. These real time clocks are used to initialise the system clock at startup. A suitably privileged user can set the system clock using the **clock** command as follows:

`switch#`**`clock set <hh:mm:ss day month year>`** where hh;mm;ss is 24 hour time, day is the current date, month and year are the name of the month and year in full, e.g, *clock set 08:52:00 8 February 2005.*

Installing the Fabric Manager

The Cisco Fabric Manager is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3). The Fabric Manager application is not required but is an optional component in the evaluated configuration. If the administrator of the MDS switch wishes to only use the CLI for configuration, monitoring and troubleshooting, they are still operating within the evaluated configuration without Fabric Manager.

In the evaluated configuration the administrator must communicate with the Cisco Fabric Manger over HTTPS. To configure Cisco Fabric Manger for HTTPS access, see:

http://www.cisco.com/univercd/cc/td/doc/product/sn5000/mds9000/3_0/fmcfg/part01/wc.htm#wp598823

The Cisco Fabric Manager applications are:

- Fabric Manager Client: Provides a graphical user interface (GUI) that displays real-time views of your network fabric, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches.

- Fabric Manager Server: Performs advanced monitoring, troubleshooting, and configuration for multiple fabrics. It must be started before running the Fabric Manager Client. It can be accessed by up to 16 Fabric Manager Clients at a time.
- Device Manager: Presents two views of a switch.
- Device View: Displays a continuously updated physical representation of the switch configuration, and provides access to statistics and configuration information for a single switch.

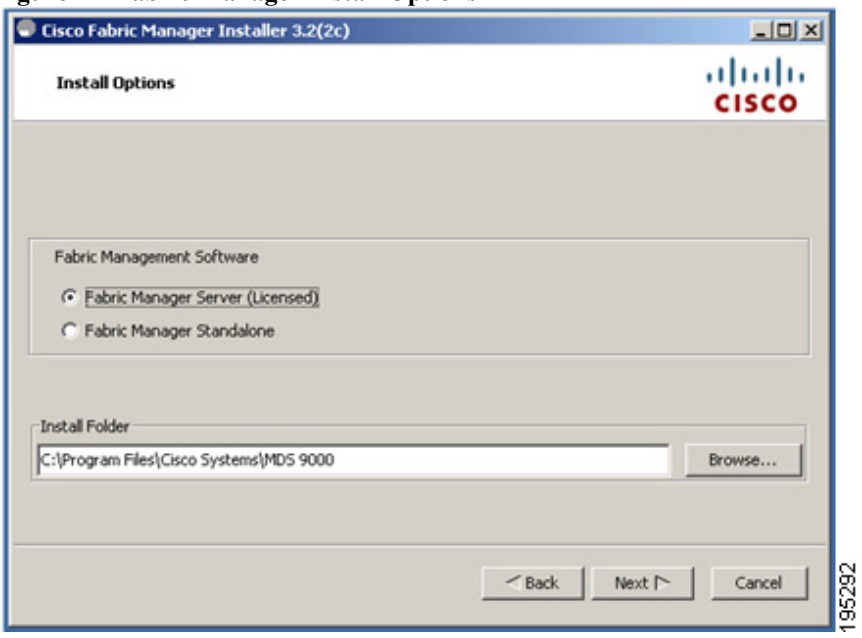
The Cisco Fabric Manager applications are an alternative to the CLI for most switch configuration commands.

NOTE: The evaluated configuration requires the administrator to manually raise the log level for the Fabric Manager Server to include audit information for login and logout operations. To modify the TOE to comply with this guidance, open "log4j_fms.xml". This is stored in "\Program Files\Cisco Systems\MDS 9000\conf" on Windows machines and in /usr/local/cisco_mds9000/conf or $HOME/cisco_mds9000/conf on UNIX systems (both Linux and Solaris), depending on the permissions of the user doing the installation. Search for INFO and change the "Web client log file" and the "Web Client logging" sections to DEBUG.

SEE: *Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 4.x* **[3]** for detailed instructions for installation of the Fabric Manger.

NOTE: When installing Fabric Manager, Standalone installation is not supported in the evaluated configuration (see **Figure 2 Fabric Manager Install Options**, below).

Figure 2 Fabric Manager Install Options



NOTE: On the Database Options screen of the Fabric Manager Installation wizard, when setting the communication parameters for the PostgreSQL database, the "DB User" field should be set

to a value other than standard administrator titles, and the "DB Password" field should be set to a value that is at least eight characters long, contains both upper and lower case characters, contains at least 1 special character (`~!@#$%^&*()-_=+), contains at least one number (0-9), and meets the rest of the complexity requirements from the Security Management Section above. This database is protected by the host operating system.

NOTE: When installing Fabric Manager all authentication modes (Local, RADIUS, TACACS or MDS) are supported in the evaluated configuration. See "Installing Fabric Manager" section in Chapter 2 of the Fabric Manager Configuration Guide. Also, the following table indicates the privilege distribution based on the authentication mode chosen.

Table 8 FM Authentication and Privilege Division

network-admin(sw)	network-operator(sw)	network-admin(fm)	network-operator(fm)	Permission	FM Client auth modes	CLI auth modes	DM auth modes	FM Web auth modes
Yes				• Create, modify and delete switch user accounts	All	All	All	
Yes				• Create and assign switch security roles	All	All	All	
Yes				• Change the default security parameters	All	All	All	
Yes				• Specify CLI session and shell timeout periods	All	All		
Yes				• View logged in switch users	All	All		
Yes				• Logout a switch user	All	All		
Yes				• Bind entities to a fibre channel port	All	All	All	
Yes				• Bind inter-switch links within a VSAN	All	All	All	
Yes				• Add or remove switches, hosts and/or devices to the fabric	All	All	All	
Yes				• Create and modify IP-based ACLs to restrict management traffic	All	All	All	
Yes				• Configure ACLs between devices and user groups within the same VSAN	All	All	All	
Yes				• Configure RADIUS and TACACS+ parameters on the switch	All	All	All	
Yes	Yes			• Review audit events on the switch	All	All	All	

network-admin(sw)	network-operator(sw)	network-admin(fm)	network-operator(fm)	Permission	FM Client auth modes	CLI auth modes	DM auth modes	FM Web auth modes
Yes		Yes		• Create, modify and delete FM user accounts	All			All
Yes		Yes		• View logged in FM Client users	All			All
Yes		Yes		• Logout an FM Client user	All			All
Yes		Yes		• Add or Remove a fabric from the list of monitored fabrics	All			All
Yes		Yes		• Create and assign FM security roles				All
Yes	Yes	Yes		• View zone, VSAN, and Fabric Membership	All	All		All
Yes		Yes		• Configure RADIUS and TACACS+ parameters on the FM				All
Yes		Yes		• Review FM Server logs				All
		Yes		• Configure initial database communication parameters				All
		Yes	Yes	• View the TOE configuration (on the FM) including Health, Performance, Inventory and Custom Reports for fabrics that have already been discovered.				Local only

A local FM Username and password is configured during installation (see example Windows screenshot in Figure **3** below). Note that if MDS or RADIUS/TACAS+ authentication is selected and the switches or servers are not available the authentication will fail over to local authentication from the Fabric Manager local database. The authentication setting (as MDS or RADIUS/TACAS+) is not altered, though. The failover settings for Fabric Manager are shown in Table 9 below.

Figure 3 Local FM User

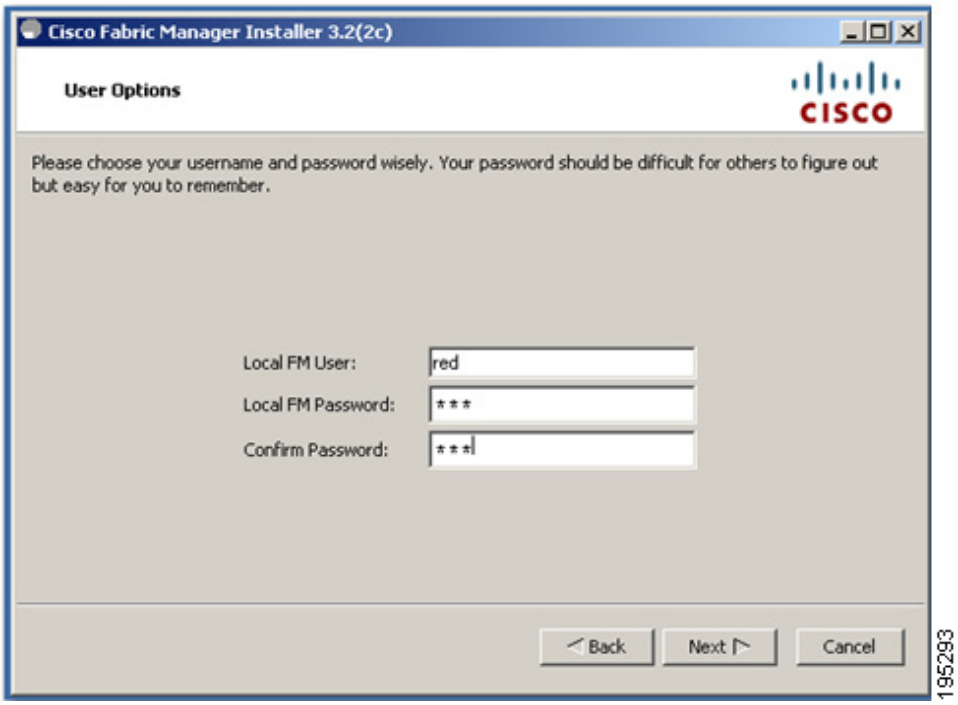
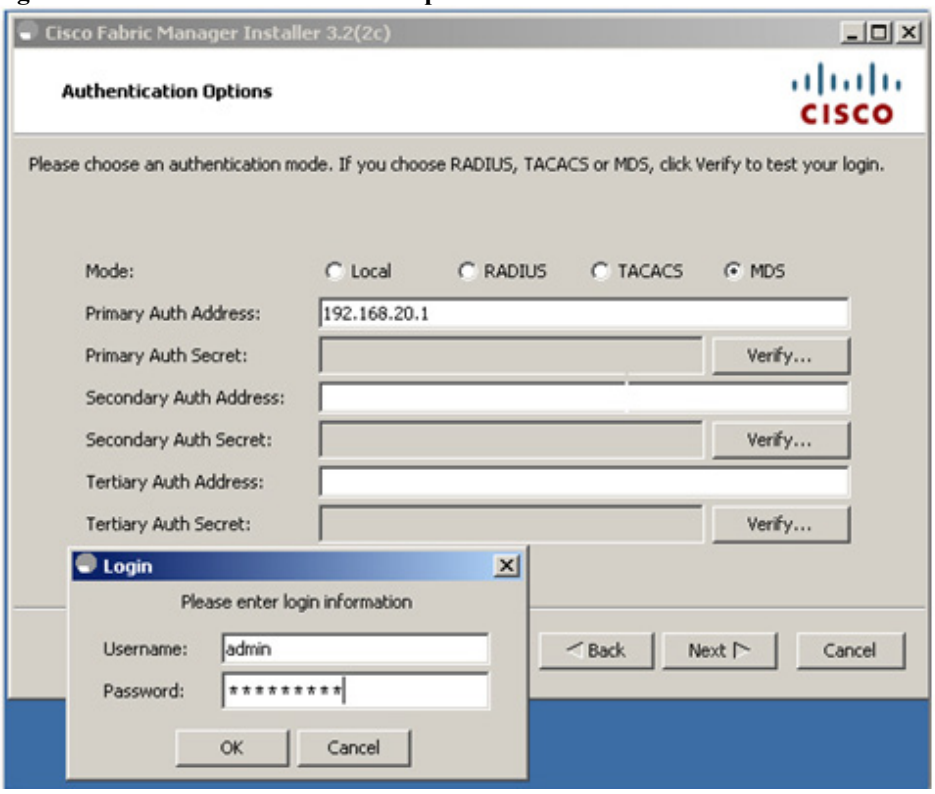


Table 9 Authentication Fallback Capabilities

MDS	network-admin(sw)	Command Line Interface	None
		Fabric Manager Web Client	Local network-admin(FM) credentials if none of the authentication switches are available
		Fabric Manager Client	Local network-admin(FM) credentials if none of the authentication switches are available. This will only open the client, however. The network-admin(sw) credentials must be provided to discover new fabrics.
		Device Manager	None
MDS	network-operator(sw)	Command Line Interface, Fabric Manager Client, Device Manager	Local network-admin(FM) credentials if none of the authentication switches are available with the exception of Device Manager, which has no fallback.
MDS	network-admin(FM)	Fabric Manager Web Client	None (This is the role that is used for fallback.)
		Fabric Manager Client	

MDS	network-operator(FM)	No interface available	N/A
Local	network-admin(sw)	Command Line Interface	None
		Device Manager	None
Local	network-operator(sw)	Command Line Interface	None
Local	network-admin(FM)	Fabric Manager Web Client	None
		Fabric Manager Client	None
Local	network-operator(FM)	Fabric Manager Web Client	None
RADIUS/ TACACS+	network-admin(sw)	Command Line Interface	None
		Fabric Manager Web Client	Local network-admin(FM) credentials if none of the authentication servers are available
		Fabric Manager Client	Local network-admin(FM) credentials if none of the authentication servers are available
		Device Manager	None
RADIUS/ TACACS+	network-operator(sw)	Command Line Interface, Fabric Manager Client, Device Manager	Local network-admin(FM) credentials if none of the authentication servers are available with the exception of Device Manager, which has no fallback.
RADIUS/ TACACS+	network-admin(FM) S	Fabric Manager Web Client	None (This is the role that is used for fallback.)
		Fabric Manager Client	
RADIUS/ TACACS+	network-operator(FM)	Fabric Manager Web Client	None

Figure 4 MDS Authentication Example



Securing the Fabric Manager Installation

The following configuration changes must be applied for secure operation of the TOE:

Securing PostgreSQL, version 8.2.4

The TOE evaluated configuration requires that the PostgreSQL is disabled from allowing connections from remote hosts and only listen on the host OS local loopback address.

For Windows installations:

Chdir to C:\Program Files\PostgreSQL\8.2\data

For UNIX installations the path is:

/var/lib/pgsql/data

Edit the postgresql.conf file

Change the lines:

```
listen_addresses = '*' to listen_addresses = 'localhost'
```

Restart the PostgreSQL service.

Securing JBoss 4.2.2

The TOE evaluated configuration requires that the JBoss JMX Console and Web Console are disabled. In order to disable the JMX Console and Web Console follow these steps:

For Windows installations:

chdir to C:\Program Files\Cisco Systems\MDS 9000\jboss\server\default\deploy\

rename jmx-console.war to jmx-console.war.bak

chdir to C:\Program Files\Cisco Systems\MDS 9000\jboss\server\default\deploy\management\console-mgr.sar\

rename web-console.war to web-console.war.bak

restart Fabric Manager

For UNIX installations the paths are:

/usr/local/cisco_mds9000/jboss/server/default/deploy/

/usr/local/cisco_mds9000/jboss/server/default/management/console-mgr.sar/

Command Line Interfaces to Installed Database

While operating in the evaluated configuration the TOE administrator shall not use any available command line interfaces to the postgresSQL database.

MD5 Hash Values for NX-OS Release 4.1(3a) Software Images

Table 10 MD5 Hash Values for NX-OS Release 4.1(3a) Software Images

Image Name	Description	MD5 Hash of NX-OS Image
m9500-sf2ek9-kickstart-mz.4.1.3a.bin	Kickstart image for Cisco MDS 9500 Series Directors for Supervisor 2	c24c41645eb895bd695b50959b2b0e48
m9500-sf2ek9-mz.4.1.3a.bin	System image for Cisco MDS 9500 Series Directors for Supervisor 2	4441a2b99f5a617e90cbb3e8960e1c76
m9200-ek9-kickstart-mz.4.1.3a.bin	Kickstart image for Cisco MDS 9216 Series Fabric Switches	fc00d84309b347db0a811ec6273f372d
m9200-ek9-mz.4.1.3a.bin	System image for Cisco MDS 9216 Series Fabric Switches	986d0768abbd6e7e2cdcdd5e5e2eb604
m9100-s2ek9-kickstart-mz.4.1.3a.bin	Kickstart image for Cisco MDS 9120 and 9140 Fabric Switches	73dea155017947b7a454b0e92b026bf5
m9100-s2ek9-mz.4.1.3a.bin	System image for Cisco MDS 9120 and 9140 Fabric Switches	6a607043330eecabbdf6d641b39069f0
m9000-cd-4.1.3a.zip	Cisco MDS 9000 Family Management Software and Documentation CD-ROM Image	cf53574ab1e2953fae5bc34c2e94aa55

This can be used to verify the authenticity of this document. Further verification of MD5 hash values can be obtained by contacting Cisco Technical support.

Related Documentation

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly “What’s New in Cisco Product Documentation,” which lists all new and revised Cisco technical documentation at:

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

You can also access the most current Cisco documentation on the World Wide Web at the following sites:

http://www.cisco.com

http://www-china.cisco.com

http://www-europe.cisco.com

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. For more information on doing so see:

http://www.cisco.com/web/siteassets/contacts/td_feedback.html

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883
USA

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center (TAC)

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3: Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4: You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to:

http://www.cisco.com/web/partners/pr11/pr193/application.html

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

P1 and P2 level problems are defined as follows:

- P1: Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2: Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.