New and Changed Information

This document provides release-specific information for each new and changed feature in Cisco Storage Media Encryption.

The *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide* applies to Cisco NX-OS Release 4.1(3), but includes all features in Cisco SAN-OS releases. If you are running Cisco SAN-OS 3.x or lower software on an MDS switch, refer to the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide* for the release train that applies to the release on your switch.

Note As of NX-OS Release 4.1(1c), SAN-OS has been changed to NX-OS. References to SAN-OS releases before 4.1(1c) still apply.

To check for additional information about this release, refer to the *Cisco MDS 9000 Family Release Notes* available at the following Cisco Systems website:

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

Table 1 summarizes the new and changed features as described in the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*, each supported Cisco MDS SAN-OS release and NX-OS release for the Cisco MDS 9500 Series, with the latest release first. The table includes a brief description of each new feature and the release in which the change occurred.

Table 1 New and Changed Features for Cisco Storage Media Encryption

Feature	GUI Change	Description	Changed in Release	Where Documented
SSN-16	The Interfaces table in the FM GUI displays four SME interfaces instead of one.	The Cisco MDS 9000 Family 16-Port Storage Services Node is a new hardware which provides a high performance unified platform for deploying enterprise-class disaster recovery and business continuance solutions with future support for intelligent fabric applications.	4.2(1)	Chapter 1, “Product Overview” Chapter 2, “Getting Started” Chapter 3, “Cisco SME Interface Configuration”
SME scalability		Enhancements in the infrastructure to ensure better scalability.	4.1(3)	Chapter 1, “Product Overview”

Table 1 New and Changed Features for Cisco Storage Media Encryption (continued)

Feature	GUI Change	Description	Changed in Release	Where Documented
High Availability KMC server	HA settings available on the Key Manager Settings page. Primary and secondary servers can be chosen during cluster creation. Primary and secondary server settings can be modified in the Cluster detail page.	High availability KMC can be configured by using a primary and secondary servers.	4.1(3)	Chapter 1, "Product Overview" Chapter 4, "Cisco SME Cluster Management" Chapter 6, "Cisco SME Key Management"
Auto replication of media keys	Remote replication relationship settings available.	A remote replication relationship can be set between volume groups. Cisco SME allows you to automatically replicate the media keys from one Cisco SME cluster to one or more clusters.	4.1(3)	Chapter 6, "Cisco SME Key Management"
Troubleshooting scenarios		Two troubleshooting scenarios added.	4.1(3)	Chapter 9, "Cisco SME Troubleshooting"
Migrating Cisco SME database tables		A database migration utility transfers the contents from one database to another.	4.1(3)	Appendix G, "Migrating Cisco SME Database Tables"
Host names are accepted as server addresses		You can enter IP addresses or host names for the servers.	4.1(3)	Chapter 4, "Cisco SME Cluster Management" Chapter 6, "Cisco SME Key Management"
RKM Migration procedure		Procedure to migrate from Cisco KMC to RKM is explained.	4.1(1c)	Appendix D, "RSA Key Manager and Cisco SME"
Software change		As of Release 4.1(1b) and later, the MDS SAN-OS software is changed to MDS NX-OS software. The earlier releases are unchanged and all refrerences are retained.	4.1(1c)	All chapters
Cisco SME roles		Added the Cisco Storage Administrator and Cisco SME KMC Administrator roles.	4.1(1c)	Chapter 1, "Product Overview"
Key Management		The Cisco KMC can be separated from Fabric Manager for multisite deployments.	4.1(1c)	Chapter 1, "Product Overview"
FC-Redirect and CFS Regions		Support for CFS Regions and Cisco SME available.	4.1(1c)	Chapter 2, "Getting Started"
Migrating KMC Server		KMC server can be migrated.	4.1(1c)	Chapter 6, "Cisco SME Key Management"

Table 1 New and Changed Features for Cisco Storage Media Encryption (continued)

Feature	GUI Change	Description	Changed in Release	Where Documented
Key Manager Settings	A new option 'None' is added to the Key Manager Settings page in the Fabric Manager web client.	A key manager needs to be selected before configuring Cisco SME. There are three options for key manager available now.	4.1(1c)	Chapter 2, "Getting Started"
feature command		Use the **feature** command to enable or disable Cisco SME feature.	4.1(1c)	Appendix A, "SME Commands"
Generating and Installing Self-Signed Certificates		How to configure SSL when KMC is separated from Fabric Manager Server.	4.1(1c)	Appendix C, "Provisioning Self-Sign Certificates"
Accounting Log	Updated accounting log messages Accounting Log information	Users can view the rekey operations and their status in the SME tab of the Fabric Manager Web Client.	4.1(1c) 3.3(1c)	Chapter 6, "Cisco SME Key Management"
Target-Based Load Balancing		Clustering offers target-based load balancing of Cisco SME services.	3.3(1c)	Chapter 1, "Product Overview"
Enabling Clustering Using Fabric Manager	Change in Command menu of the Control tab.	Users can select **enable** to enable clustering.	3.3(1c)	Chapter 2, "Getting Started"
Enabling Cisco SME Using Fabric Manager	Change in Command menu of the Control tab.	Users can select **enable** to enable the Cisco SME feature.	3.3(1c)	Chapter 2, "Getting Started"
Enabling SSH Using Fabric Manager	Error dialog box in Fabric Manager	An error message dialog box displays if the Fabric Manager GUI is used to enable SSH before using the Device Manager or the CLI to generate the SSH keys.	3.3(1c)	Chapter 2, "Getting Started"
Enabling SSH Using Device Manager	SSH Telnet windows	Users should first create and then enable SSH using Device Manager.	3.3(1c)	Chapter 2, "Getting Started"
Transport Settings	New step in the Cisco SME wizard for creating a cluster.	Allows users to enable or disable transport settings for Cisco SME.	3.3(1c)	Chapter 4, "Cisco SME Cluster Management"
Configuring and Starting Cisco SME Interface	Create SME Interfaces window	Users should create Cisco SME interfaces using Device Manager or the CLI, before using the Fabric Manager to create the interfaces.	3.3(1c)	Chapter 3, "Cisco SME Interface Configuration"
Volume Key Rekey	Rekey tab added in the Volume Groups tab of the Fabric Manager Web Client.	Volume keys are rekeyed to ensure better security or when key security is compromised.	3.3(1c)	Chapter 6, "Cisco SME Key Management"

Table 1 New and Changed Features for Cisco Storage Media Encryption (continued)

Feature	GUI Change	Description	Changed in Release	Where Documented
Master Key Rekey	Storing new master keyshares in the smart cards.	In the advanced mode, the smart card replacement triggers a master key rekey and a new version of the master key is generated for the cluster. The new set of master keyshares are stored in the smart cards. All the volume group keys are also synchronized with the new master key.	3.3(1c)	Chapter 6, "Cisco SME Key Management"
Load-Balancing Command		Describes the command that enables cluster reloading for all targets or specific targets.	3.3(1c)	Appendix A, "Cisco SME CLI Commands"
Secure Sockets Layer (SSL) Command		Describes the command that enables SSL.	3.3(1c)	Appendix A, "Cisco SME CLI Commands"
Offline Data Restore Tool (ODRT) Command		Describes the Linux-based command that invokes the ODRT application.	3.3(1c)	Appendix A, "Cisco SME CLI Commands"
Offline Data Restore Tool (ODRT) application		Describes the ODRT solution for recovering encrypted data on tape volume groups when the MSM-18/4 module or the Cisco MDS 9222i switch is unavailable.	3.3(1c)	Appendix B, "Offline Data Recovery in Cisco SME"
Introduction to Secure Sockey Layer (SSL)		Describes how to configure SSL for Cisco SME and edit SSL settings in the Cisco SME wizard.	3.3(1c)	Appendix C, "Provisioning Self-Sign Certificates"
Database Backup and Restore		Describes how to back up and restore Fabric Manager Server databases.	3.3(1c)	Appendix E, "Database Backup and Restore"