



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

Table 1 lists 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*

Feature	GUI Change	Description	Changed in Release	Where Documented
Write signature	New feature	This is a new feature on the signature cluster mode.	5.2(6)	Chapter 6, “Configuring SME Disks.”
Snapshot support	New feature	This is a new feature and two types of snapshot are supported.	5.2(6)	Chapter 6, “Configuring SME Disks.”
Rekeying	New feature	This is a new feature and is a special function of the data preparation operation.	5.2(6)	Chapter 6, “Configuring SME Disks.”
SME Disk	New feature.	This is a new feature that encrypts the data contained in a disk.	5.2(1)	Chapter 6, “Configuring SME Disks”
SME scalability	Updates	For disks, batching is automatically enabled.	5.2(1)	“SME CLI Commands”
Disk Key Replication (DKR) feature	New	Is used to manage crypto keys of disks involved in a replication relationship.	5.2(1)	
16-port Storage Services Node (SSN-16) module	The Interfaces table in the Fabric Manager GUI displays four SME interfaces instead of one.	The Cisco MDS 9000 Family 16-Port Storage Services Node is new hardware that 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, “Storage Media Encryption Overview” Chapter 2, “Configuring SME” Chapter 3, “Configuring SME Interfaces”

Table 1 **New and Changed Features (continued)**

Feature	GUI Change	Description	Changed in Release	Where Documented
SME scalability	New feature.	Use the scaling batch enable command to enable scaling in SME.	4.1(3)	“SME CLI Commands”
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, “Storage Media Encryption Overview” Chapter 4, “Configuring SME Cluster Management” Chapter 7, “Configuring SME Key Management”
Auto replication of media keys	Replication relationship settings are available.	Remote replication relationships can be set between volume groups. SME allows you to automatically replicate the media keys from one SME cluster to one or more clusters. Auto replication of media keys is only applicable for SME Tapes.	4.1(3)	Chapter 7, “Configuring SME Key Management”
Troubleshooting scenarios		Two troubleshooting scenarios added.	4.1(3)	Chapter 11, “SME Troubleshooting”
Migrating SME database tables		A database migration utility transfers the contents from one database to another.	4.1(3)	Appendix Q, “Migrating 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, “Configuring SME Cluster Management” Chapter 7, “Configuring SME Key Management”
RKM Migration procedure		Procedure to migrate from Cisco KMC to RKM is explained. RKM is only supported on SME Tape.	4.1(1c)	“RSA Key Manager and SME”

Table 1 **New and Changed Features (continued)**

Feature	GUI Change	Description	Changed in Release	Where Documented
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 references are retained.	4.1(1c)	All chapters
SME roles		Added the Cisco Storage Administrator and SME KMC Administrator roles.	4.1(1c)	Chapter 1, “Storage Media Encryption Overview”
Key Management		The Cisco KMC can be separated from Fabric Manager for multisite deployments.	4.1(1c)	Chapter 1, “Storage Media Encryption Overview”
FC-Redirect and CFS Regions		Support for CFS Regions and SME available.	4.1(1c)	Chapter 2, “Configuring SME”
Migrating KMC Server		KMC server can be migrated.	4.1(1c)	Chapter 7, “Configuring SME Key Management”
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 SME. There are three options for key manager available now.	4.1(1c)	Chapter 2, “Configuring SME”
feature command		Use the feature command to enable or disable SME feature.	4.1(1c)	“SME CLI Commands”
Generating and Installing Self-Signed Certificates		How to configure SSL when KMC is separated from Fabric Manager Server.	4.1(1c)	“Provisioning 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 7, “Configuring SME Key Management”
Target-Based Load Balancing		Clustering offers target-based load balancing of SME services.	3.3(1c)	Chapter 1, “Storage Media Encryption 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, “Configuring SME”
Enabling SME Using Fabric Manager	Change in Command menu of the Control tab.	Users can select enable to enable the SME feature.	3.3(1c)	Chapter 2, “Configuring SME”

Table 1 **New and Changed Features (continued)**

Feature	GUI Change	Description	Changed in Release	Where Documented
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, “Configuring SME”
Enabling SSH Using Device Manager	SSH Telnet windows	Users should first create and then enable SSH using Device Manager.	3.3(1c)	Chapter 2, “Configuring SME”
Transport Settings	New step in the SME wizard for creating a cluster.	Allows users to enable or disable transport settings for SME.	3.3(1c)	Chapter 4, “Configuring SME Cluster Management”
Configuring and Starting SME Interface	Create SME Interfaces window	Users should create SME interfaces using Device Manager or the CLI, before using the Fabric Manager to create the interfaces.	3.3(1c)	Chapter 3, “Configuring SME Interfaces”
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. Volume key rekey is only applicable to SME Tapes.	3.3(1c)	Chapter 7, “Configuring SME Key Management”
Master Key Rekey	Storing new master keyshares in the smart cards.	In SME disk cluster, with the advanced mode, the smart card replacement triggers a master key rekey and a new version of the master key is generated for the disk cluster. The new set of master keyshares are stored in the smart cards.	5.2(1)	Chapter 7, “Configuring SME Key Management”
		In SME tape cluster, with 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)	

Table 1 **New and Changed Features (continued)**

Feature	GUI Change	Description	Changed in Release	Where Documented
Load-Balancing Command		Describes the command that enables cluster reloading for all targets or specific targets.	3.3(1c)	“SME CLI Commands”
Secure Sockets Layer (SSL) Command		Describes the command that enables SSL.	3.3(1c)	“SME CLI Commands”
Offline Data Restore Tool (ODRT) Command		Describes the Linux-based command that invokes the ODRT application. The offline data restore tool command is only applicable for SME tapes.	3.3(1c)	“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, SSN-16 module, or the Cisco MDS 9222i switch is unavailable. The offline data restore tool application is only applicable for SME tapes.	3.3(1c)	“Offline Data Recovery in SME”
Introduction to Secure Socket Layer (SSL)		Describes how to configure SSL for SME and edit SSL settings in the SME wizard.	3.3(1c)	“Provisioning Certificates”
Database Backup and Restore		Describes how to back up and restore Fabric Manager Server databases.	3.3(1c)	“Database Backup and Restore”

Send documentation comments to mdsfeedback-doc@cisco.com