

New and Changed Information

Feature Name	Description	Release	Where Documented
show ssl info	Support for viewing the SSL version was added.	8.4(2)	SSH Authentication Using Digital Certificates
Custom Roles	Support for creating custom roles was added. The **attribute-admin** keyword was added for the **rule** command.	8.3(1)	Configuring Role Modification by Custom Roles
LDAP Enhancements	LDAP connections on port 636 automatically start securely with SSL or TLS.	8.2(1)	Configuring Remote LDAP Server Profiles

• New and Changed Information, on page 1

New and Changed Information

Feature Name	Description	Release	Where Documented
OIDC/OAuth2 Authentication	Support has been introduced for user authentication by OAuth2/OIDC. This enhances switch access security by integrating with centralized identity providers and supporting MFA and SSO.	9.4(5)	OIDC/OAuth2 Authentication
PKI Certificate Management	Support has been introduced for Enrollment over Secure Transport (EST) X.509 certificate	9.4(5)	PKI Certificate Management

Feature Name	Description	Release	Where Documented
	management. This allows secure and automated certificate provisioning and renewal on switches.		
TACACS+Over TLS	Support has been introduced for CFS distribution of TACACS over TLS configuration.	9.4(5)	TACACS+ Over TLS
AES-256 encryption for SNMP	Support for AES-256 encryption key for SNMP has been added.	9.4(4)	Configuring SNMP
TACACS+Over TLS	TACACS+ over TLS is a secure method for centralized Authentication, Authorization, and Accounting (AAA) supported on Cisco MDS switches.	9.4(3b)	TACACS+ Over TLS
FC-SP Encryption Key Size	Support to allow 256 bits for encryption key is added. The switch(config-sa)# encryption command has been introduced in configuration mode.	9.4(3)	About Cisco TrustSec FC Link Encryption
Custom SSH Cryptographic Algorithms	You can configure support for SSH key exchange algorithms, message authentication codes (MACs), key types, and ciphers.	9.4(1)	Customizing SSH Cryptographic Algorithms