



New and Changed Information

This chapter includes the new and changed features for the Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.6(x).

- [New and Changed Information, on page 1](#)

New and Changed Information

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Securing NX-OS with Cisco Live Protect	This feature protects the Nexus switches in monitoring mode, and is implemented using the NXSecure configuration.	10.6(1)F	Secure NX-OS with Cisco Live Protect
MACsec support on Cisco Nexus 9336C-SE1 switch	Added MACsec support on Cisco Nexus 9336C-SE1 switches.	10.6(1)F	Guidelines and limitations for MACsec on Cisco Nexus 9336C-SE1 switches
Custom CoPP support on Cisco Nexus 9336C-SE1 switch	Added Custom CoPP support on Cisco Nexus 9336C-SE1 switches.	10.6(1)F	Guidelines and limitations for CoPP on Cisco Nexus 9336C-SE1 switches
ACL support on Cisco Nexus 9336C-SE1 switch	Cisco Nexus 9336C-SE1 switches support these ACL features: • PACL • RACL on L3 interfaces, L3 Port-channel interfaces, subinterfaces, and SVI interfaces • PBR ACL	10.6(1)F	Guidelines and Limitations for IP ACLs

Feature	Description	Changed in Release	Where Documented
TACACS+ over TLS	Added support to configure TACACS+ over TLS	10.6(1)F	Guidelines and Limitations for TACACS+ Configuring TACACS+ Over TLS Verifying TACACS+ Over TLS Configuration
Host Identity Based Authorization (HIBA)	Added support for centralized SSH authorization management by embedding host authorization information within certificates.	10.6(1)F	SSH Authentication Using Host Identity Based Authorization (HIBA) Configuring HIBA for SSH Authentication
Deprecate redundant SSH configuration and DSA CLIs	Added support to deprecate redundant SSH configuration and DSA CLIs	10.6(1)F	Guidelines and Limitations for SSH and Telnet Generating SSH Server Keys Configuring SSH Passwordless File Copy