

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
Secure NX-OS with Live Protect enhancements	Enhancements supported are • policy mode can now be specified while adding policy to the switch • syslog is supported now, and • a new show command is introduced to display the log history for a particular policy.	10.6(3)F	Live Protect Guidelines and limitations for Live Protect Add or remove Live Protect policy packages Verify policy status for Live Protect System log support
MACsec ND ISSU	Added support ND ISSU on Nexus 9300-FX, FX2, and FX3 switches when MACsec is enabled	10.6(3)F	Guidelines and limitations for MACsec

Feature	Description	Changed in Release	Where Documented
Support for 802.1X authentication mode open on MDA ports	Added support for open authentication mode to provide immediate network access for quick connectivity but still maintain security by running authentication in parallel.	10.6(3)F	Open mode Guidelines and limitations of 802.1x for voice VLAN Configure 802.1x open mode and restrict violation action on an interface 802.1X port configuration commands
Support command for 802.1X authentication violation restrict	Added a new command to handle security violations by creating DROP entries for violating MAC addresses instead of shutting down the port.	10.6(3)F	Violation restrict mode Guidelines and limitations of 802.1x for voice VLAN Configure 802.1x open mode and restrict violation action on an interface 802.1X port configuration commands
Support Change of Authorization (COA) for Voice and Data traffic	Added support for COA to enable real-time authorization updates from ISE without client disconnection.	10.6(3)F	Guidelines and limitations of 802.1x for voice VLAN
Support Dynamic ACL for Voice VLAN and Data VLAN	Added support for DACL multi-domain mode to provide granular per-client traffic control with rules specific to each MAC address and VLAN.	10.6(3)F	DACL for multi-domain mode Guidelines and limitations of 802.1x for voice VLAN
AAA, RADIUS, and TACACS+ support on Cisco Nexus 9164E-NS4-O switch	Cisco Nexus 9164E-NS4-O switches support AAA, RADIUS, and TACACS+ features.	10.6(2n)	chapter4.pdf#nameddest=unique_24 unique_24_Connect_42_spectrum Guidelines and limitations for RADIUS on Cisco Nexus 9164E-NS4-O switches Guidelines and limitations for TACACS+ on Cisco Nexus 9164E-NS4-O switches
CoPP support on Cisco Nexus 9164E-NS4-O switch	Added CoPP support on Nexus 9164E-NS4-O switches.	10.6(2n)	Guidelines and limitations for CoPP on Cisco Nexus 9164E-NS4-O switches:

Feature	Description	Changed in Release	Where Documented
ACL support on Cisco Nexus 9164E-NS4-O switch	Cisco Nexus 9164E-NS4-O switches support RACL and QoS on Layer 3 interfaces.	10.6(2n)	cisco-nexus-9000-series-nx-os-security-configuration-guide-10x_chapter12.pdf#nameddest=unique_28 unique_28_Connect_42_spectrum
Live Protect support on N9164E-NS4-O switch	Added support for Live Protect feature on N9164E-NS4-O switch	10.6(2n)	Guidelines and limitations for Live Protect
DHCP relay support on Cisco Nexus 9164E-NS4-O switch	Added DHCP relay support on Cisco Nexus 9164E-NS4-O switches.	10.6(2n)	Guidelines and limitations for DHCP relay on Cisco Nexus 9164E-NS4-O switches
MACsec ND ISSU	Two new commands are introduced at the MACsec policy level to support MACsec ND ISSU on Cisco Nexus 9300-GX2, H2R and H1 switches.	10.6(2)F	Guidelines and limitations for MACsec Configure a MACsec policy MACsec configuration verification commands
AAA, RADIUS, TACACS+, and SSH protocol	Cisco N9324C-SE1U and N9348Y2C6D-SE1U Smart switches support AAA, RADIUS, TACACS+, and SSH protocol features.	10.6(2)F	Guidelines and limitations for AAA on Cisco N9300 smart switches Guidelines and limitations for RADIUS on Cisco N9300 smart switches Guidelines and limitations for TACACS+ on Cisco N9300 smart switches Guidelines and limitations for SSH protocol on Cisco N9300 smart switches
MACsec support on Cisco N9300 Smart switch	Added MACsec support on Cisco N9300 Smart switches.	10.6(2)F	Cisco N9300 Smart switch limitations
Custom CoPP support on Cisco N9300 Smart switch	Added Custom CoPP support on Cisco N9300 Smart switches.	10.6(2)F	Guidelines and limitations for CoPP on Cisco N9300 smart switches

Feature	Description	Changed in Release	Where Documented
ACL support on Cisco N9300 Smart switch	Cisco N9300 Smart switches support these ACL features: • PACL • RACL on L3 interfaces, L3 Port-channel interfaces, subinterfaces, and SVI interfaces • PBR ACL	10.6(2)F	ACL guidelines and limitations for Cisco N9300 Smart switches
DHCP relay support on Cisco N9300 Smart switch	Added DHCP relay support on Cisco N9300 Smart switches.	10.6(2)F	Guidelines and limitations for DHCP relay on Cisco N9300 smart switches
Live Protect supported on Smart switches	Added support for Live Protect on N9324C-SE1U and N9348Y2C6D-SE1U Smart switches	10.6(2)F	Live Protect
Enforce Mode support for Live Protect	Added support for enforce mode as part of the Live Protect feature	10.6(2)F	Live Protect Guidelines and limitations for Live Protect Add or remove Live Protect policy packages Verify policy status for Live Protect Modify the policy mode
Routing TACACS+ (AAA) Traffic via Linux Kernel Network Stack	Beginning with Cisco NX-OS Release 10.6(2)F, Cisco Nexus 9000 Series switches support routing TACACS+ (AAA) traffic via the Linux kernel network stack (kstack) in addition to the existing netstack path.	10.6(2)F	Guidelines and Limitations for TACACS+

Feature	Description	Changed in Release	Where Documented
DHCP Relay to Server in Local Guest Shell/Docker	Beginning with Cisco NX-OS Release 10.6(2), Cisco Nexus 9000 switches support relaying DHCP requests to a server running locally within the switch, either in the Guest Shell or as a Docker container. This capability allows the switch to forward DHCP client requests received on its interfaces to a locally hosted DHCP server, enabling centralized and flexible IP address assignment within the network environment.	10.6(2)F	DHCP relay to server in local guest shell/docker Relay DHCP packets to a local guest shell or docker DHCP server Guidelines and limitations Configure DHCP relay to local guest shell/docker Verify DHCP relay to local guest shell/docker
Displaying Cisco SUDI Certificate Chain	Beginning with Cisco NX-OS Release 10.6(2), Cisco Nexus 9000 switches support displaying and signing the Cisco Secure Unique Device Identifier (SUDI) certificate chain as part of Cisco's trustworthy technologies, which leverage Secure Unique Device Identifier (SUDI) and Trust Anchor Module (TAm). This capability allows the switch to display the SUDI certificate chain and generate a signature based on a user-provided nonce, supporting integration with external systems.	10.6(2)F	Displaying Cisco SUDI certificate chain How SUDI certificate chain display and signing works Guidelines and limitations Verify SUDI certificate
Cisco Discovery Protocol (CDP) enhancement for second port disconnect	Added CDP enhancement for second Port disconnect which allows a Cisco IP phone to send a CDP message to a switch when a host is unplugged from behind the phone.	10.6(2)F	Functionalities of 802.1x for voice VLAN Guidelines and limitations of 802.1x for voice VLAN
MAC move support for data clients on MDA ports	Added support to handle MAC move events for data clients connected to Multi-Domain Authentication (MDA) ports.	10.6(2)F	Functionalities of 802.1x for voice VLAN

Feature	Description	Changed in Release	Where Documented
Support for 1R2C on Cisco N9300 Series smart switches	Added 1R2C support for traffic storm control on Cisco N9300 Series smart switches.	10.6(2)F	Guidelines and limitations for traffic storm control Configure traffic storm control for one-level threshold on N9300 series smart switches
RACL on SVI	Added RACL support on SVI interfaces of Cisco Nexus 9364E-SG2 Series switches.	10.6(2)F	Guidelines and limitations for IP ACLs
Securing NX-OS with 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 Live Protect
MACsec support on Cisco Nexus 9336C-SE1 switch	Added MACsec support on Cisco Nexus 9336C-SE1 switches.	10.6(1)F	Cisco Nexus 9336C-SE1 switch limitations
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
TACACS+ over TLS	Added support to configure TACACS+ over TLS	10.6(1)F	Guidelines and limitations for TACACS+ Configure TACACS+ over TLS TACACS+ over TLS configuration verification

Feature	Description	Changed in Release	Where Documented
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) Configure 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 Configure SSH passwordless file copy

New and Changed Information