New and Changed Information

This chapter contains the following sections:

- New and Changed Information, on page 1

New and Changed Information

The following tables provide an overview of the significant changes to this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco APIC Release 6.0 (4)

Feature or Change	Description	Where Documented
N/A	This document has no changes from the previous release.	N/A

Table 2: New Features and Changed Information for Cisco APIC Release 6.0(3)

Feature	Description	Where Documented
TCP MSS adjustment	You can adjust the transmission control protocol (TCP) maximum segment size (MSS) to avoid packet fragmentation or drops.	About TCP MSS Adjustment

Feature	Description	Where Documented
Rogue endpoint exception list support for bridge domains and L3Outs	You can create a global rogue/COOP exception list, which excludes a MAC address from rogue endpoint control on all the bridge domains on which the MAC address is discovered, and you can create a rogue/COOP exception list for L3Outs. You can also exclude all MAC addresses for a bridge domain or L3Out. This simplifies creating the exception list when you want to make an exception for every MAC address; you do not need to enter each address individually.	About the Rogue/COOP Exception List

Table 3: New Features and Changed Behavior in Cisco APIC Release 6.0 (2)

Feature or Change	Description	Where Documented
N/A	This document has no changes from the previous release.	N/A

Table 4: New Features and Changed Information for Cisco APIC Release 6.0(1)

Feature	Description	Where Documented
Cisco Nexus 9000 switch secure erase	Cisco Nexus 9000 switches utilize persistent storage to maintain system software images, switch configuration, software logs, and operational history. Each of these areas can contain user-specific information such as details on network architecture and design, and potential target vectors for would-be attackers. The secure erase feature enables you comprehensively to erase this information, which you can do when you return a switch with return merchandise authorization (RMA), upgrade or replace a switch, or decommission a system that has reached its end-of-life.	About Cisco Nexus 9000 Switch Secure Erase