



## New and Changed Information

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

## New and Changed Information

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release.

**Table 1: New and Changed Security Features**

Feature	Description	Changed in Release	Where Documented
Control Plane Policing	Added the functionality to classify and rate-limit IP unicast RPF failure packets.	6.2(10)	<a href="#">Configuring Control Plane Policing</a>
ACL TCAM bank mapping	Added a command to display the bank mapping matrix.	6.2(10)	<a href="#">Configuring IP ACLs</a>
Cisco TrustSec	Added SGT support for F3 Series modules.	6.2(10)	Configuring Cisco TrustSec
DHCP relay trusted interfaces	Added support for the following commands: <ul style="list-style-type: none"> <li>• <b>ip dhcp relay information option trust</b></li> <li>• <b>ip dhcp relay information trusted</b></li> <li>• <b>ip dhcp relay information trust-all</b></li> </ul>	6.2(8)	<a href="#">Configuring DHCP</a>
Cisco TrustSec	Enabled MACSec support for F2e modules. Added support for batching SGACL programming tasks.	6.2(6)	Configuring Cisco TrustSec
Cisco TrustSec	Added the ability to map VLANs to SGTs.	6.2(2)	Configuring Cisco TrustSec

Feature	Description	Changed in Release	Where Documented
Cisco TrustSec	Added the ability to encrypt the SAP PMK and display the PMK in encrypted format in the running configuration.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the <b>show cts sap pmk</b> command to display the hexadecimal value of the configured PMK.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the <b>show cts capability interface</b> command to display the Cisco TrustSec capability of interfaces.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Enabled the <b>cts sgt</b> , <b>policy static sgt</b> , and <b>clear cts policy sgt</b> commands to accept decimal values.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the ability to download sname tables from ISE and to refresh the environment data manually and upon environment data timer expiry.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added optional keywords to the <b>show cts role-based sgt-map</b> command to display a summary of the SGT mappings or the SGT map configuration for a specific SXP peer, VLAN, or VRF.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the <b>brief</b> keyword to the <b>show cts interface</b> command to display a brief summary for all CTS-enabled interfaces.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added SGT support for F2 and F2e Series modules.	6.2(2)	Configuring Cisco TrustSec
CoPP	Updated the output of the <b>show policy-map interface control-plane</b> command to show the 5-minute moving averages and peaks of the conformed and violated byte counts for each policy in each module.	6.2(2)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Added VRRP6 ACL support to police VRRP IPv6 traffic. The HSRP ACL is modified to reflect the correct destination addresses of control packets.	6.2(2)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Changed the behavior of multicast traffic from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates.	6.2(2)	<a href="#">Configuring Control Plane Policing</a>

Feature	Description	Changed in Release	Where Documented
CoPP	Added the ability to monitor CoPP with SNMP.	6.2(2)	<a href="#">Configuring Control Plane Policing</a>
DHCP	Added support for the DHCPv6 relay agent.	6.2(2)	<a href="#">Configuring DHCP</a>
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	<a href="#">Configuring IP ACLs</a>
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	<a href="#">Configuring IP ACLs</a>
Rate limits	Added support for Layer 3 glean fast-path packets.	6.2(2)	<a href="#">Configuring Rate Limits</a>
VLAN ACLs	Added support for deny ACEs in a sequence.	6.1(3)	<a href="#">Configuring VLAN ACLs</a>
Cisco TrustSec	Removed the requirement for the Advanced Services license.	6.1(1)	<a href="#">Configuring Cisco TrustSec</a>
Cisco TrustSec	Added MACsec support for 40G and 100G M2 Series modules.	6.1(1)	<a href="#">Configuring Cisco TrustSec</a>
CoPP	Added a new class for FCoE; added the LISP, LISP6, and MAC Layer 3 IS-IS ACLs to the critical class; added the fcoe-fib-miss match exception to the undesirable class; added the MAC Layer 2 tunnel ACL to the Layer 2 unpoliced class, and added the "permit icmp any any 143" rule to the acl-icmp6-msgs ACL.	6.1(1)	<a href="#">Configuring Control Plane Policing</a>
FIPS	Added support for digital image signing on switches that contain the Supervisor 2 module.	6.1(1)	<a href="#">Configuring FIPS</a>
FIPS	Updated FIPS guidelines for M2 Series modules.	6.1(1)	<a href="#">Configuring FIPS</a>
IP ACLs and MAC ACLs	Updated for M2 Series modules.	6.1(1)	<a href="#">Configuring IP ACLs and Configuring MAC ACLs</a>
Cisco TrustSec	Updated for F2 Series modules.	6.0(1)	<a href="#">Configuring Cisco TrustSec</a>
CoPP	Added the dense default CoPP policy.	6.0(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Added the ability to configure the CoPP scale factor per line card.	6.0(1)	<a href="#">Configuring Control Plane Policing</a>
FIPS	Updated FIPS guidelines for F2 Series modules.	6.0(1)	<a href="#">Configuring FIPS</a>

Feature	Description	Changed in Release	Where Documented
IP ACLs, MAC ACLs, and VACLs	Updated for F2 Series modules.	6.0(1)	<a href="#">Configuring IP ACLs</a> , <a href="#">Configuring MAC ACLs</a> , and <a href="#">Configuring VLAN ACLs</a>
Rate limits	Added support for F2 Series modules.	6.0(1)	<a href="#">Configuring Rate Limits</a>
RBAC	Added support for F2 Series modules.	6.0(1)	<a href="#">Configuring User Accounts and RBAC</a>
TACACS+	Added the ability to configure command authorization for a console session.	6.0(1)	<a href="#">Configuring TACACS+</a>
User accounts and RBAC	Added the ability to configure a read-only or read-and-write rule for an SNMP OID.	6.0(1)	<a href="#">Configuring User Accounts and RBAC</a>
ACLs and CoPP	Changed the <b>show running-config aclmgr</b> and <b>show startup-config aclmgr</b> commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.	5.2(1)	<a href="#">Configuring IP ACLs</a> , <a href="#">Configuring MAC ACLs</a> , <a href="#">Configuring VLAN ACLs</a> , and <a href="#">Configuring Control Plane Policing</a>
Cisco TrustSec	Added support for pause frame encryption and decryption on interfaces.	5.2(1)	<a href="#">Configuring Cisco TrustSec</a>
CoPP	Added the ability to change or reapply the default CoPP policy without rerunning the setup utility.	5.2(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Changed the CoPP best practice policy to read-only and added the ability to copy the policy in order to modify it.	5.2(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Added the <b>show copp profile</b> and <b>show copp diff profile</b> commands to display the details of the CoPP best practice policy and the differences between policies, respectively.	5.2(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Changed the <b>show copp status</b> command to display which flavor of the CoPP best practice policy is attached to the control plane.	5.2(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Changed the name of the <b>none</b> option for the best practices CoPP profile in the setup utility to <b>skip</b> .	5.2(1)	<a href="#">Configuring Control Plane Policing</a>

Feature	Description	Changed in Release	Where Documented
CoPP	Updated the default class maps with support for MPLS LDP, MPLS OAM, MPLS RSVP, DHCP relay, and OTV-AS.	5.2(1)	<a href="#">Configuring Control Plane Policing</a>
DHCP	Added subnet broadcast support for the DHCP relay agent and support for DHCP smart relay.	5.2(1)	<a href="#">Configuring DHCP</a>
FCoE ACLs	Added support for FCoE ACLs on F1 Series modules.	5.2(1)	<a href="#">Configuring IP ACLs</a>
IP ACLs	Added support for ACL capture on M1 Series modules.	5.2(1)	<a href="#">Configuring IP ACLs</a>
LDAP	Deprecated the <b>ldap-server port</b> command.	5.2(1)	<a href="#">Configuring LDAP</a>
Password encryption	Added support for AES password encryption and a configurable master encryption key.	5.2(1)	<a href="#">Configuring Password Encryption</a>
RADIUS	Added type-6 encryption support for RADIUS server keys.	5.2(1)	<a href="#">Configuring RADIUS</a>
TACACS+	Added type-6 encryption support for TACACS+ server keys.	5.2(1)	<a href="#">Configuring TACACS+</a>
Control plane policy map	Added the ability to specify the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold.	5.1(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Updated the default policies with the 802.1Q class of service (cos) values.	5.1(1)	<a href="#">Configuring Control Plane Policing</a>
CoPP	Added support for non-IP traffic classes.	5.1(1)	<a href="#">Configuring Control Plane Policing</a>
DHCP snooping	Optimized DHCP snooping to work in a vPC environment.	5.1(1)	<a href="#">Configuring DHCP</a>
FIPS	Added the ability to configure Federal Information Processing Standards (FIPS) mode.	5.1(1)	<a href="#">Configuring FIPS</a>
Rate limits	Added support for F1 Series module packets.	5.1(1)	<a href="#">Configuring Rate Limits</a>
Rate limits	Added the ability to configure rate limits for packets that reach the supervisor module and to log a system message if the rate limit is exceeded.	5.1(1)	<a href="#">Configuring Rate Limits</a>
Rate limits	Added options to disable rate limits and to configure rate limits for a specific module and port range.	5.1(1)	<a href="#">Configuring Rate Limits</a>

Feature	Description	Changed in Release	Where Documented
SCP and SFTP servers	Added the ability to configure SCP and SFTP servers on the Cisco NX-OS device to support the copy of files to and from a remote device.	5.1(1)	<a href="#">Configuring SSH and Telnet</a>
User roles	Added the ability to display the syntax of the commands that the network-admin and network-operator roles can use.	5.1(1)	<a href="#">Configuring User Accounts and RBAC</a>
VTY ACLs	Added support to control access to traffic received over a VTY line.	5.1(1)	<a href="#">Configuring IP ACLs</a>
802.1X	Supports configuring 802.1X on member ports of a port channel.	5.0(2)	<a href="#">Configuring 802.1X</a>
AAA authorization	Supports configuring the default AAA authorization method for TACACS+ servers.	5.0(2)	<a href="#">Configuring TACACS+</a>
CHAP authentication	Allows the enabling or disabling of CHAP authentication.	5.0(2)	<a href="#">Configuring AAA</a>
CoPP	Updated the default policies with support for ACL HSRP6.	5.0(2)	<a href="#">Configuring Control Plane Policing</a>
DHCP	Allows the DHCP relay agent to support VRFs. Also adds the <b>ip dhcp relay information option vpn</b> command and modifies the <b>ip dhcp relay address</b> command.	5.0(2)	<a href="#">Configuring DHCP</a>
DHCP	Supports enabling DHCP to use Cisco proprietary numbers 150, 152, and 151 for the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.	5.0(2)	<a href="#">Configuring DHCP</a>
IP ACLs, MAC ACLs, and VACLs	Allows up to 128K ACL entries when using an XL line card, provided a scalable services license is installed.	5.0(2)	<a href="#">Configuring IP ACLs</a> , <a href="#">Configuring MAC ACLs</a> , and <a href="#">Configuring VLAN ACLs</a>
LDAP	Supports configuring the Lightweight Directory Access Protocol (LDAP).	5.0(2)	<a href="#">Configuring LDAP</a>
Local authentication	Enables fallback to local authentication when remote authentication fails.	5.0(2)	<a href="#">Configuring AAA</a>
Local authentication	Allows the disabling of fallback to local authentication.	5.0(2)	<a href="#">Configuring AAA</a>
OTP	Supports one-time passwords.	5.0(2)	<a href="#">Configuring RADIUS</a>

Feature	Description	Changed in Release	Where Documented
Periodic server monitoring	Supports global periodic RADIUS and TACACS+ server monitoring.	5.0(2)	<a href="#">Configuring RADIUS and Configuring TACACS+</a>
PKI	Supports a remote cert-store and certificate mapping filters.	5.0(2)	<a href="#">Configuring PKI</a>
Privilege roles	Supports permitting or denying commands for users of privilege roles.	5.0(2)	<a href="#">Configuring TACACS+</a>
Rate limits	Supports Layer 2 Tunnel Protocol (L2TP) packets.	5.0(2)	<a href="#">Configuring Rate Limits</a>
SGACL policies	Allows the enabling or disabling of RBACL logging.	5.0(2)	<a href="#">Configuring Cisco TrustSec</a>
SGACL policies	Allows the enabling, disabling, monitoring, and clearing of RBACL statistics.	5.0(2)	<a href="#">Configuring Cisco TrustSec</a>
SSH	Supports configuring a maximum number of SSH login attempts.	5.0(2)	<a href="#">Configuring SSH and Telnet</a>
SSH	Supports starting SSH sessions from the boot mode of a Cisco NX-OS device in order to connect to a remote device.	5.0(2)	<a href="#">Configuring SSH and Telnet</a>
SSH	Supports copying files from a Cisco NX-OS device to an SCP or SFTP server without a password.	5.0(2)	<a href="#">Configuring SSH and Telnet</a>
TACACS+ privilege-level authorization	Supports the mapping of privilege levels configured for users on the TACACS+ server to locally configured user roles on the Cisco NX-OS device.	5.0(2)	<a href="#">Configuring TACACS+</a>

