



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
SGACL Detailed Logging	Support for Cisco Nexus M2 and M3 series modules is introduced.	7.3(1)D1(1)	Configuring Cisco TrustSec
Configuring IP ACLs over M3 modules	Support for Cisco Nexus M3 modules is introduced.	7.3(0)DX(1)	Configuring IP ACLs
Login Block Per User	Added support for login block per user.	7.3(0)D1(1)	Configuring AAA
SGACL ACLLOGs	Added the functionality to enable SGACL logging.	7.3(0)D1(1)	Configuring Cisco TrustSec
SGACL Monitoring	Added the functionality to enable monitoring of the SGACLs.	7.3(0)D1(1)	Configuring Cisco TrustSec
SXPv3	Added the support for the SGT Exchange Protocol Version 3.	7.3(0)D1(1)	Configuring Cisco TrustSec
Cisco TrustSec Subnet to SGT Mapping	Added the support for the Cisco TrustSec Subnet to SGT Mapping.	7.3(0)D1(1)	Configuring Cisco TrustSec
Lightweight DHCPv6 Relay Agent	Added the support for the Lightweight DHCPv6 Relay Agent.	7.3(0)D1(1)	Configuring DHCP
UDP Relay	Added the support for the UDP relay feature.	7.3(0)D1(1)	Configuring DHCP

Feature	Description	Changed in Release	Where Documented
Flexible ACL TCAM Bank Chaining	Added the support for the flexible ACL TCAM bank chaining feature.	7.3(0)D1(1)	Configuring IP ACLs
Cisco TrustSec MACsec over FabricPath on F3	Added support for Cisco TrustSec MACsec on F3 series modules on FabricPath.	7.2(1)D1(1)	Configuring Cisco TrustSec
Configuring Login Grace Time for SSH Connections	Added the ability to configure login grace time for SSH connections.	7.2(0)D1(1)	Configuring SSH and Telnet
Cisco TrustSec	Added support for the following: <ul style="list-style-type: none"> • Cisco TrustSec Support on Port-Channel Members • 2,00,000 IP-SGT maps • Change of Authorization • SGT with FabricPath is supported on F2E and F3 linecards • MACSec functionality on F3 linecard on classical Ethernet mode • SGT Classification via Port Profiles • SGT Support for Virtual Port Channel (vPC) and vPC+ 	7.2(0)D1(1)	Configuring Cisco TrustSec
Control Plane Policing	Added the functionality to classify and rate-limit IP unicast RPF failure packets.	6.2(10)	Configuring Control Plane Policing
ACL TCAM bank mapping	Added a command to display the bank mapping matrix.	6.2(10)	Configuring IP ACLs
Cisco TrustSec	Added SGT support for F3 Series modules.	6.2(10)	#unique_16
DHCP relay trusted interfaces	Added support for the following commands: <ul style="list-style-type: none"> • ip dhcp relay information option trust • ip dhcp relay information trusted • ip dhcp relay information trust-all 	6.2(8)	Configuring DHCP
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 show cts sap pmk command to display the hexadecimal value of the configured PMK.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the show cts capability interface command to display the Cisco TrustSec capability of interfaces.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Enabled the cts sgt , policy static sgt , and clear cts policy sqt 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 show cts role-based sgt-map 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 brief keyword to the show cts interface 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 show policy-map interface control-plane 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)	Configuring Cisco TrustSec
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)	Configuring Control Plane Policing
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)	Configuring Control Plane Policing

Feature	Description	Changed in Release	Where Documented
CoPP	Added the ability to monitor CoPP with SNMP.	6.2(2)	Configuring Control Plane Policing
DHCP	Added support for the DHCPv6 relay agent.	6.2(2)	Configuring DHCP
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	Configuring IP ACLs
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	Configuring IP ACLs
Rate limits	Added support for Layer 3 glean fast-path packets.	6.2(2)	Configuring Rate Limits
VLAN ACLs	Added support for deny ACEs in a sequence.	6.1(3)	Configuring VLAN ACLs
Cisco TrustSec	Removed the requirement for the Advanced Services license.	6.1(1)	Configuring Cisco TrustSec
Cisco TrustSec	Added MACsec support for 40G and 100G M2 Series modules.	6.1(1)	Configuring Cisco TrustSec
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)	Configuring Control Plane Policing
FIPS	Added support for digital image signing on switches that contain the Supervisor 2 module.	6.1(1)	Configuring FIPS
FIPS	Updated FIPS guidelines for M2 Series modules.	6.1(1)	Configuring FIPS
IP ACLs and MAC ACLs	Updated for M2 Series modules.	6.1(1)	Configuring IP ACLs and Configuring MAC ACLs
Cisco TrustSec	Updated for F2 Series modules.	6.0(1)	Configuring Cisco TrustSec
CoPP	Added the dense default CoPP policy.	6.0(1)	Configuring Control Plane Policing
CoPP	Added the ability to configure the CoPP scale factor per line card.	6.0(1)	Configuring Control Plane Policing
FIPS	Updated FIPS guidelines for F2 Series modules.	6.0(1)	Configuring FIPS

Feature	Description	Changed in Release	Where Documented
IP ACLs, MAC ACLs, and VACLs	Updated for F2 Series modules.	6.0(1)	Configuring IP ACLs , Configuring MAC ACLs , and Configuring VLAN ACLs
Rate limits	Added support for F2 Series modules.	6.0(1)	Configuring Rate Limits
RBAC	Added support for F2 Series modules.	6.0(1)	Configuring User Accounts and RBAC
TACACS+	Added the ability to configure command authorization for a console session.	6.0(1)	Configuring TACACS+
User accounts and RBAC	Added the ability to configure a read-only or read-and-write rule for an SNMP OID.	6.0(1)	Configuring User Accounts and RBAC

