

Cisco Secure Access and Cisco TrustSec Release 5.0 System Bulletin

Introduction

Cisco® Secure Access and Cisco TrustSec® capabilities provide an intelligent access control solution for highly secure network access. They show who and what is connecting to the network and mitigate risk through centralized controls over the resources that users and devices can access.

The flexible authentication and device-classification functions of Cisco Secure Access enable identity- and context-aware network services to be deployed in the access layer of enterprise networks. These features work with the Cisco Identity Services Engine (ISE) to validate user and device identities, profile devices and give them access to the network, and assess device postures and remediate them if necessary.

With Cisco Secure Access, access controls can be applied at the point of network access. These controls include VLAN and downloadable IP access control list (ACL) assignments.

Cisco TrustSec technology opens up a new approach to defining access controls: They can be invoked anywhere on the network or applied across a network. This capability is possible because the access controls are managed through a layer of abstraction that decouples the security rules and policies from the network devices that apply them.

- Cisco TrustSec functions can be applied to user-accessed networks, data center infrastructure, routers, and security appliances.
- Cisco TrustSec technology simplifies the provision of access controls and segmentation functions through the use of logical identifiers called security group tags (SGTs). These can be used anywhere on the network, because they work independently of the underlying IP address or VLAN mechanisms traditionally used for access control.

Cisco Secure Access provides baseline network access authentication and enforces detailed user-identity-based policies for network access. Cisco TrustSec functions simplify the provisioning and management of access control policies after the user or device is granted access to the network.

To help smooth customer deployments of the complete solution, Cisco has developed a rigorous validation process that encompasses component-level interoperability, scalability, and performance tests.

Summary of New Cisco TrustSec Capabilities

One of the major advantages of the Cisco TrustSec solution is that it allows customers to apply policy-defined segmentation functions, with the policy elements decoupled from the underlying network topology. With version 5.0 of the solution:

- Cisco TrustSec policy-enforcement capabilities are extended on new switching platforms, so that enterprise customers can enforce consistent policies across campus and branch networks.

-
- Cisco TrustSec capabilities continue to support Cisco Connected Grid Switches and Routers as well as the Cisco Industrial Ethernet switch families, delivering policy-enforcement capabilities to field locations for energy providers and utilities.
 - Access policies can be assigned consistently to any method of accessing the enterprise network, whether it is wired, wireless, or remote access.

The Cisco TrustSec 5.0 release continues to validate three major use cases:

- Access to data centers, to help organizations gain visibility into, and effective control over, unmanaged mobile devices accessing network services and company data.
- Campus network segmentation, to allow organizations to set access policies based on the user or device role, instead of a logical topology such as VLAN or subnet. This use case is also validated by Verizon Business, as a means to reduce the audit scope for Payment Card Industry Data Security Standard (PCI-DSS) regulatory requirements.
- Servers in a data center can be segmented for security policy compliance as well. Segmentation between virtual instances of servers and physical servers, or among physical servers, allows organization to accelerate their service provisioning much faster, while maintaining security policy more easily.

New Cisco TrustSec Features Validated in Release 5.0

- Inline SGT tagging capabilities are now supported by Cisco Catalyst[®] 3850 Series and 3650 Series Switches, Cisco Catalyst 4500 Supervisor Engine 7-E and 7L-E, Cisco Catalyst 4500-X Series Switches, Catalyst 6800-X Series Switches along with the Cisco Catalyst 6800ia Instant Access switch, and the Cisco 5760 Wireless LAN Controller (WLC). These platforms support receiving and sending SGT-embedded Layer 2 frames on built-in Gigabit Ethernet ports. SGT information can thus be exchanged with directly connected peers without using the SGT Exchange Protocol (SXP).
- Security group ACL (SG-ACL) capabilities are supported by Cisco Catalyst 3850 and 3650 Series Switches, Cisco Catalyst 4500 Supervisor Engine 7-E and 7L-E, Catalyst 4500-X Series Switch, and Catalyst 6800-X Series Switches along with the Cisco Catalyst 6800ia Instant Access switch, and the Cisco 5760 WLC. These platforms now support traffic enforcement based on SGTs. User and device segmentation can be applied across the campus network, including traffic within a same VLAN or across multiple VLANs. Enforcement capability is also available in the unified wireless and wired network when Cisco Catalyst 3850, Cisco Catalyst 3650 switches or 5760 WLC switches are used.
- Both the Cisco 4451-X Integrated Services Router and the Cisco Cloud Services Router (CSR) 1000V Series have been added to the supported-device list. Features such as Security Group Firewall, Security Exchange Protocol version 4, and SGT over GETVPN link are now supported on those platforms.
- Newly introduced Catalyst switches support SXP version 4, including the Cisco Catalyst 2960-X, 2960-XR, 3650, 3850, and 4500-X Series Switches, and Cisco Catalyst 4500 Supervisor Engine 8-E and Cisco Catalyst 6800ia Switch.
- SXP is now supported by Cisco Industrial Ethernet 2000 and 3000 Series Switches and Cisco 2500 Series Connected Grid Switches.
- Cisco ASA 5500-X Series Next-Generation Firewalls now support security group classification for SSL and IPsec VPN sessions for remote access users, along with Cisco ISE 1.2. In addition, IP-to-SGT mapping information for remote access sessions can be propagated using SXP, which is already supported in the Cisco ASA 9.0 release.

- The Cisco TrustSec solution is validated with Cisco ISE 1.2.

Product Components and Features

Table 1 summarizes the latest platforms and features that are validated in Cisco Secure Access and Cisco TrustSec 5.0. A complete list is available at: cisco.com/go/TrustSec.

Table 1. Cisco TrustSec Platform Support Matrix

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Identity Services Engine	Cisco ISE 3315, 3355, 3395, 3415, and 3495; appliances and VMware	Cisco ISE 1.0	Cisco ISE 1.2 Patch 5 (requires Advanced license)	–	–	–	–
Cisco Catalyst® 2000 Series	Cisco Catalyst 2960-Plus Series Switches (LAN Base required)	Cisco IOS® Software Release 15.2(1)E1	-	Dynamic, IP to SGT, VLAN to SGT Subnet to SGT	S v2	No	No
	Cisco Catalyst 2960-C Series (LAN Base required)	Cisco IOS Software Release 15.0(1)SE2	-	Dynamic, IP to SGT, VLAN to SGT Subnet to SGT	S v2	No	No
	Cisco Catalyst 2960-S and 2960-SF Series (LAN Base required)	Cisco IOS Software Release 15.0(1)SE2	Cisco IOS Software Release 15.0(2)SE2	Dynamic, IP to SGT, VLAN to SGT Subnet to SGT	S v2	No	No
	Cisco Catalyst 2960-X and 2960-XR Series (LAN Base required)	Cisco IOS Software Release 15.0(2)EX1	Cisco IOS Software Release 15.0(2)EX4	Dynamic, IP to SGT, VLAN to SGT Subnet to SGT	S v3	No	No
	Cisco Catalyst 3000 Series	Cisco Catalyst 3560-E and 3750-E Series (IP Base required)	Cisco IOS Software Release 15.0(1)SE2	Cisco IOS Software Release 15.0(2)SE5	Dynamic, IP to SGT, VLAN to SGT	S, L v2	No
	Cisco Catalyst 3560-C Series (IP Base required)	Cisco IOS Software Release 15.0(1)SE2	Cisco IOS Software Release 15.0(1)SE2	Dynamic, IP to SGT, VLAN to SGT	S, L v2	No	No
	Cisco Catalyst 3560-X and 3750-X Series (IP Base required)	Cisco IOS Software Release 15.0(2)SE	Cisco IOS Software Release 15.2(1)E1	Dynamic, IP to SGT, VLAN to SGT	S, L v2	SGT over Ethernet, SGT over MACsec (with fixed port & C3KX-SM-10G)	SG-ACL
	Cisco Catalyst 3650 and 3850 Series (IP Base required)	Cisco IOS XE 3.3.1SE	Cisco IOS XE 3.3.1SE	Dynamic, IP to SGT, VLAN to SGT, port to SGT, subnet to SGT	S, L v4	SGT over Ethernet (MACsec in future release)	SG-ACL

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Catalyst 4000 Series	Cisco Catalyst 4500 Supervisor Engine 6-E and 6L-E (IP Base required)	Cisco IOS Software Release 15.1.(1)SG	Cisco IOS Software Release 15.1.(1)SG	Dynamic, IP to SGT, VLAN to SGT	S, L v2	No	No
	Cisco Catalyst 4500 Supervisor Engine 7-E and 7L-E (IP Base required)	Cisco IOS XE 3.3.0SG	Cisco IOS XE 3.5.1E	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT, Layer 3 Interface (L3IF) to SGT	S, L v4	SGT over Ethernet, SGT over MACsec (See footnote for list of supported line cards)	SG-ACL
	Cisco Catalyst 4500 Supervisor Engine 8-E (IP Base required)	Cisco IOS XE 3.3.0X0	Cisco IOS XE 3.3.0X0	Dynamic, IP to SGT, VLAN to SGT, port to SGT, Subnet to SGT	S, L v4	No	No
	Cisco Catalyst 4500-X Series (IP Base required)	Cisco IOS XE 3.3.0SG	Cisco IOS XE 3.5.1E	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT	S, L v4	SGT over Ethernet, SGT over MACsec	SG-ACL
Cisco Catalyst 6500 Series	Cisco Catalyst 6500 Series Supervisor Engine 32 and 720 (IP Base required)	Cisco IOS 12.2(33)SXJ2	Cisco IOS Software Release 12.2(33)SXJ2	Dynamic, IP to SGT	S, L v2	No	No
	Cisco Catalyst 6500 Series Supervisor Engine 2T (IP Base required)	Cisco IOS Software Release 15.0(1)SY1	Cisco IOS Software Release 15.1(2)SY1	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT, L3IF-to-SGT	S, L v4	SGT over Ethernet, SGT over MACsec (requires WS-X6900 line card for both features)	SG-ACL
	Cisco Catalyst 6800-X and 6800ia (IP Base required)	Cisco IOS Software Release 15.0(1)SY1	Cisco IOS Software Release 15.1(2)SY1	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT, L3IF to SGT	S, L v4	SGT over Ethernet, SGT over MACsec (requires WS-X6900 for Catalyst 6807)	SG-ACL
Cisco Connected Grid Routers and Switches	Cisco 2010 Connected Grid Routers	Cisco IOS Software Release 15.3(2)T	Cisco IOS Software Release 15.4(1)T	Dynamic, IP to SGT, VLAN to SGT	S, L v4	SGT over Ethernet, SGT over GETVPN or IPsecVPN	SG Firewall
	Cisco 2500 Series Connected Grid Switches	Cisco IOS Software Release 15.0(1)SE2	Cisco IOS Software Release 15.0(2)EK1	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT	S, L v3	No	No
Cisco Industrial Ethernet Switches	Cisco IE 2000 Series	Cisco IOS Software Release 15.0(2)EB	-	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT	S v2 (available as of 15.2(1)EY)	No	No
	Cisco IE 3000 Series	Cisco IOS Software Release 15.2(1)EY	Cisco IOS Software Release 15.2(1)EY	Dynamic, IP to SGT, VLAN to SGT, subnet to SGT	S, L v4	No	No

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco Wireless Controllers	Cisco 5500 Series and 2500 Series; Cisco Wireless Services Module 2 (WiSM2); and Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2) (WLC 7500, 8500 and vWLC do not support Cisco TrustSec)	Cisco AireOS 7.4	Cisco AireOS 7.6.100.0	Dynamic	S v2	No	No
	Cisco 5760 Wireless LAN Controller	Cisco IOS XE 3.2.1SE	Cisco IOS XE 3.3.1SE	Dynamic, IP to SGT, VLAN to SGT, port to SGT, subnet to SGT	S, L v4	SGT over Ethernet	SG-ACL (requires Cisco IOS XE 3.3.1 SE)
Cisco Nexus® 7000 Series	All Cisco Nexus 7000 line cards and chassis	Cisco NX-OS Software 6.1(1) (SGT support in Base license 6.1 and later)	Cisco NX-OS Software 6.2(6)	Static IP to SGT, L2IF to SGT, port Profile to SGT, VLAN to SGT	S, L v1	SGT over Ethernet, SGT over MACsec (supported on all line cards except F1 and F2 line cards)	SG-ACL
Cisco Nexus 5000 Series	Cisco Nexus 5548P, 5548UP, and 5596UP (Note: No support for 5010 or 5020)	Cisco NX-OS Software 5.1(3)N1	Cisco NX-OS Software 6.0(2)N2(2)	L2IF to SGT	S v1	SGT over Ethernet (no MACsec option)	SG-ACL
Cisco Nexus 1000V	Cisco Nexus 1000V	Cisco NX-OS Software 4.2(1)SV2(1.1) with Advanced feature license	Cisco NX-OS Software 4.2(1)SV2(1.1) with Advanced feature license	IP to SGT, port profile to SGT	S v1	No	No
Cisco Integrated Services Router (ISR) G2	Cisco 890, 1900, 2900, 3900 Series	Cisco IOS Software Release 15.2(2)T	Cisco IOS Software Release 15.4(1)T1	Dynamic, IP to SGT	S, L v4	SGT over Ethernet (no support on ISR G2-Cisco 800 Series), SGT over GETVPN or IPsec VPN	SG Firewall
	Cisco 4451-X ISR	Cisco IOS XE 3.11.0S	Cisco IOS XE 3.11.0S	Dynamic, IP to SGT	S, L v4	SGT over Ethernet, SGT over GETVPN or IPsec VPN	SG Firewall
	Cisco SM-X Layer 2/3 EtherSwitch Module	Cisco IOS Software Release 15.0(2)SE5	Cisco IOS Software Release 15.0(2)SE5	Dynamic, IP to SGT, VLAN to SGT	S, L v2	SGT over Ethernet, SGT over MACsec	SG-ACL
	Cisco Cloud Services Router 1000V Series	Cisco IOS XE 3.11.0S	-	Static IP to SGT	S, L v4	SGT over Ethernet, SGT over IPsec VPN	SG Firewall

System Component	Platform	Solution Minimum Version	Solution-Level Validated Version	Security Group Tag (SGT) Classification	SGT Exchange Protocol (SXP) Support and Version	Inline SGT Tagging	SGT Enforcement
Cisco ASR 1000 Series Aggregation Services Routers	Cisco ASR 1000 Series Router Processor 1 or 2 (RP1/RP2); ASR 1001, 1002, 1004, 1006, and 1013 Routers with Embedded Services Processor (10, 20, or 40 Gbps) and SPA Interface Processor (10/40)	Cisco IOS-XE 3.5	Cisco IOS XE 3.11.0S	Static IP to SGT	S, L v4	SGT over Ethernet, SGT over GETVPN or IPsec VPN	SG Firewall
Cisco ASA 5500 and 5500-X Series	Cisco ASA 5505, 5510, 5512-X, 5515-X, 5520, 5525-X, 5540, 5545-X, 5550, 5555-X, 5580, 5585-X, and ASA Services Module	Cisco ASA 9.0.1, Adaptive Security Device Manager (ASDM) 7.0.1	ASA 9.2.1, ASDM 7.1.5.100, Cisco Security .. Manager**	Dynamic, IP to SGT (for remote access only)	S, L v2	No	SG Firewall

Notes

* Product part numbers of supported line cards for SGT over Ethernet on the Cisco Catalyst 4500 Supervisor Engine 7-E and Supervise Engine 7L-E include the following: WS-X4712-SFP+E, WS-X4748-UPOE+E, WS-X4748-RJ45V+E, WS-X4748-RJ45-E, WS-X4640-CSP-E, WS-X4724-SFP-E, WS-X4748-SFP-E.

** Cisco Security manager 4.5 supports upto ASA v9.1.3 and does not support ASA v9.2.1.

Solution-level validated versions may not always represent the latest available platform version. Please visit <http://www.cisco.com> to find the latest version.

"Solution Minimum Version" indicates the earliest software or OS version for each platform that has all the necessary features for Cisco TrustSec solution support.

Dynamic classification includes SGT classification based on 802.1X authentication, MAC Authentication Bypass (MAB), or web authentication.

For SXP roles, "S" represents Speaker and "L" represents Listener.

IP to SGT, VLANto SGT, subnet to SGT, port profile to SGT, L2IF to SGT, and L3IF to SGT all use the static classification method.

For Cisco TrustSec classification, propagation, and enforcement, an IP Base K9 license is required for Cisco Catalyst 3560, 3560-E, 3750, 3750-E, 3560-C, 3560-X, 3750-X, 4500 Sup6(L)-E, 4500 Sup7(L)-E, 6500 Sup720, and 6500 Sup2T.

The Cisco ISR Base/K9 license is required for Secure Access features. For Cisco TrustSec classification, propagation, and enforcement, an ISR SEC/K9 license is required.

A Cisco ASR1000 SEC-FW license is required for ASR 1000 Series routers for all Cisco TrustSec functions.

The list of platforms validated for Secure Access features in Cisco ISE Network Component Compatibility Release 1.2 can be found at: http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/compatibility/ise_sdt.html.

Table 2 provides a list of Cisco IOS Software-based Secure Access functionalities validated in the Cisco TrustSec program. Table 3 provides the Cisco TrustSec IEEE 802.1AE (MACsec) Platform Support Matrix.

Table 2. Baseline Cisco Secure Access Functionalities and Platform Support Matrix

Cisco TrustSec Release Number	Secure Access Feature
Cisco TrustSec 1.99	802.1X authentication
	MAC Authentication Bypass
	Open access
	Flexible authentication
	Single-host mode
	Multihost mode
	Multidomain authentication mode (MDA)
	Multiauthentication mode
	VLAN assignment
	Downloadable ACL
	Inactivity timer (MAB and 802.1X)
	Local web authentication (LWA)
	Wake on LAN
	CDP second-port disconnect
	Integration with Dynamic ARP Inspection, IP Source Guard, port security
	MDA with dynamic voice VLAN assignment
	Filter-ID
	RADIUS-supplied timeout
	Guest VLAN
	Authentication-failed VLAN
RADIUS accounting	
Critical port/inaccessible authentication bypass (IAB) for data domain	
Conditional logging and debugging on per-port basis	
Cisco TrustSec 2.0	RADIUS Change of Authorization (CoA) (Catalyst 2000, 3000, and 6000 Series; Wireless LAN Controller)
	Central web authentication (CWA) (URL redirect) with Cisco ISE
Cisco TrustSec 2.1	Device sensor (Catalyst 3000 and 4000 Series; Wireless LAN Controller)
	802.1AE MACsec plus MACsec Key Agreement (Catalyst 3000-X, Catalyst 4000 Supervisor Engine 7-E)
	MAC move
	MAC replace
	Downloadable ACL enhancement
	Critical port/IAB for voice domain (Catalyst 2000, 3000, 4000, and 6000 Series)
	RADIUS CoA (Catalyst 4000 Series)
	RADIUS CoA with CWA (Wireless LAN Controller)

** Cisco ISR G2 Secure Access features have the following restrictions:

Secure Access Feature	Restriction
IEEE 802.1X with ACL enhancements	Available only on non-800 ISR G2 models
IEEE 802.1X and MAB with downloadable ACL	Available only on non-800 ISR G2 models
IEEE 802.1X and MAB with Filter-ID	Available only on non-800 ISR G2 models
IEEE 802.1X and MAB Port ACL enhancement	Available only on non-800 ISR G2 models
IEEE 802.1X and MAB with URL redirect	Available only on non-800 ISR G2 models
IEEE 802.1X and MAB with per-user ACL support	Available only on non-800 ISR G2 models
Web authentication with URL redirect	Not available on all ISR G2 platforms
Inactivity aging	Not available on all ISR G2 platforms
IEEE 802.1X user distribution	Not available on all ISR G2 platforms
IEEE 802.1X supplicant support for Message Digest 5 (MD5)	Not available on all ISR G2 platforms
IEEE 802.1x voice-aware security violations	Not available on all ISR G2 platforms
MAC-move support	Not available on all ISR G2 platforms
IEEE 802.1X readiness check	Not available on all ISR G2 platforms

Table 3. Cisco TrustSec IEEE 802.1AE (MACsec) Platform Support Matrix

System Component	Platform	Solution Minimum Version	Solution Level Validated Version	MACsec for Endpoint	Switch-to-Switch Encryption
Cisco Identity Services Engine	Cisco ISE 3315, 3355, 3395, 3415, and 3495; appliances and VMware	Cisco ISE 1.0	Cisco ISE 1.2 Patch 1 (Base license required)	Cisco ISE (required)	Cisco ISE (optional)
Cisco AnyConnect® supplicant	Network Access Module (NAM) - Hardware acceleration with Intel 82567LM Intel 82579LM	Cisco AnyConnect 3.0	Cisco AnyConnect 3.0	AnyConnect (required)	N/A
Cisco Catalyst 3000 Series	Cisco Catalyst 3560-C Series WS-C3560CG-8TC-S WS-C3560CG-8PC-S WS-C3560CDP-8PT-S	Cisco IOS Software Release 15.0(1) SE2	Cisco IOS Software Release 15.0(2)SE4	Yes (MACsec Key Agreement)	Yes (Security Association Protocol)
	Catalyst 3560-X and 3750-X <ul style="list-style-type: none"> Requires product C3KX-SM-10G for uplink (C3KX-NM-XX does not support MACsec) 	Cisco IOS Software Release 15.0(1) SE2	IOS Software Release 15.0(2)SE4	Yes (MKA)	Yes (SAP)
Cisco Catalyst 4000 Series	Cisco Catalyst 4500 (Supervisor Engine 7-E and 7L-E) <ul style="list-style-type: none"> Requires following line cards WS-X4712-SFP+E WS-X4748-UPOE+E WS-X4748-RJ45V+E WS-X4748-RJ45-E 	Cisco IOS XE 3.3.0SG	Cisco IOS XE 3.5.1E	Yes (MKA)	Yes (SAP)
	Cisco Catalyst 4500-X C4KX-NM-8SFP	Cisco IOS XE 3.5.1E	Cisco IOS XE 3.5.1E	Yes (MKA)	Yes (SAP)

System Component	Platform	Solution Minimum Version	Solution Level Validated Version	MACsec for Endpoint	Switch-to-Switch Encryption
Cisco Catalyst 6500 Series	Cisco Catalyst 6500 (Supervisor Engine 2T) <ul style="list-style-type: none"> Requires following line cards WS-X6908-10G-2T WS-X6908-10G-2TXL WS-X6904-40G-2T WS-X6904-40G-2TXL 	Cisco IOS Software Release 15.0(1)SY1	Cisco IOS Software Release 15.1(1)SY1	No	Yes (SAP)
	Cisco Catalyst 6800-X Cisco Catalyst 6880-X, 6880-X-LE Cisco Catalyst 6807 XL <ul style="list-style-type: none"> Requires following line cards WS-X6908-10G-2T WS-X6908-10G-2TXL WS-X6904-40G-2T WS-X6904-40G-2TXL Catalyst 6800ia 	Cisco IOS Software Release 15.1(2)SY1	Cisco IOS Software Release 15.1(2)SY1	No	Yes (SAP)
Cisco Nexus 7000 Series	Cisco Nexus 7x00 (Supervisor 1, 2, and 2e) <ul style="list-style-type: none"> Requires following line cards N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L N7K-M148GT-11 N7K-M148GT-11L N7K-M148GS-11 N7K-M148GS-11L N7K-M202CF-22L N7K-M206FQ-23L N7K-M224XP-23L N7K-F248XT-25E (all ports) N7K-F248XP-25E (port 41~48) 	Cisco NX-OS Software 5.2.4 Cisco NX-OS Software 6.1.1	Cisco NX-OS Software 6.2(2)	No	Yes (SAP)

Notes

System-level validated versions do not always represent the latest available platform version. Please visit <http://www.cisco.com> to find the latest version.

“Solution Minimum Version” indicates the version of code that has all the necessary features for the solution and does not indicate that this is the minimum version for individual features.

The MACsec Key Agreement Protocol is specified in IEEE802.1X-2010.

The Security Association Protocol was developed by Cisco.

A LAN Base K9 license is required for Cisco Catalyst 2960 Switches for all Secure Access features. The Cisco Catalyst 2960 LAN Lite is supported but not recommended with Cisco ISE 1.2 because of limited feature support. LAN Lite supports only 802.1X and VLAN assignments.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)