Network Access Control Capabilities of Network Devices with Cisco Identity Services Engine

Revised: July 17, 2024

Overview

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the ISE Community Resources.

Cisco ISE interoperates fully with third-party RADIUS devices that adhere to the standard protocols. Support for RADIUS functions depends on the device-specific implementation.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.

Note This document lists only the devices that are validated with Cisco ISE. Hence, this is not the complete list of devices that are supported by Cisco ISE.

The following notations are used to mark the device support:

- √ : Fully supported
- X : Not supported
- ! : Limited support, some functionalities are not supported.

Network Access Control Capabilities of Cisco Switches

Table 1: Network Access Control Capabilities of Cisco Switches

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
IE2000 IE3000	Cisco IOS 15.2(2)E4 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)EB	√	√	√	√	*X*	√	√	√
IE-3400-8P2S	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1 Cisco IOS XE 17.9.1	√	√	√	√	√	√	√	√

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
IE4000 IE5000	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IR1101-K9	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1 Cisco IOS XE 17.9.1	√	Not validated	Not validated	Not validated	Not validated	Not validated	Not validated	√
IR8340	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1	√	Not validated	Not validated	Not validated	Not validated	Not validated	Not validated	√
CGS 2520	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
Catalyst 1000	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	*X*
Catalyst 2960 LAN Base	Cisco IOS 15.0(2)SE11	√	√	√	√	*X*	√	√	*X*
	Cisco IOS v12.2(55)SE5 [4]	√	√	√	!	*X*	!	!	*X*

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
Catalyst 2960-C Catalyst 3560-C	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)EX3	√	√	√	√	√	√	√	√
Catalyst 2960-L	Cisco IOS 15.2(6.1.27)E2	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.2(6)E2	√	√	√	√	√	√	√	*X*
Catalyst 2960-Plus Catalyst 2960-SF	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)SE7	√	√	√	√	√	√	√	*X*
Catalyst 2960-CX Catalyst 3560-CX	Cisco IOS 15.2(3)E1	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(3)E	√	√	√	√	√	√	√	√
Catalyst 2960-S Catalyst 2960-XR Catalyst 2960-X	Cisco IOS 15.2.2E8	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
Catalyst 3560V2 Catalyst 3750V2	Cisco IOS 12.2(55)SE10	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560-E	Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
Catalyst 3560-G	Cisco IOS 15.0(2)SE11 Cisco IOS 15.2(2)E6 Cisco IOS 12.2(55)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560-X	Cisco IOS 15.2.4E10 Cisco IOS 15.2(4)E9 Cisco IOS 15.2(2)E6 Cisco IOS 15.2(2)E5	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3650 Catalyst 3650-X Catalyst 3850	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 3750-E Catalyst 3750-G	Cisco IOS 15.2(2) E6 Cisco IOS 12.2(55)SE5 Cisco IOS 12.2(55)SE10 Cisco IOS 12.2(55)SE11 Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
Catalyst 3750-X	Cisco IOS 15.2(2) E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 4500 Supervisor 8-E	Cisco IOS 3.11.0E ED Cisco IOS 3.10.3E Cisco IOS XE 3.6.8E Cisco IOS XE 3.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.2 XO	√	√	√	√	√	√	√	√
Catalyst 4500 Supervisor 7-E, 7L-E	Cisco IOS XE 3.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 6-E, 6L-E	Cisco IOS 15.2(2)E4	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(2)E	√	√	√	√	*X*	√	√	√
Catalyst 4500-X	Cisco IOS XE 3.6.6 E Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(6)E	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	√	√	√	√
Catalyst 5760	Cisco IOS XE 3.7.4	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
Catalyst 6500-E (Supervisor 720)	Cisco IOS 15.1(2)SY7	√	√	√	√	*X*	√	√	√
	Cisco IOS v12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (VS-S2T-10G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6807-XL Catalyst 6880-X (VS-S2T-10G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6848ia	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.1(2) SY+	√	√	√	√	*X*	√	√	√

Device	Validated OS [1]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
	Minimum OS [3]								
Cisco Catalyst 9000 series switch family including: Catalyst 9200 Catalyst 9300 Catalyst 9400 Catalyst 9500 Catalyst 9600	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1 Cisco IOS XE 17.9.1 Cisco IOS XE 17.8.1 Cisco IOS XE 17.7.1 Cisco IOS XE 17.6.1 Cisco IOS XE 17.5.1 Cisco IOS XE 17.4.1 Cisco IOS XE 17.3.1 Cisco IOS XE 17.2.1 Cisco IOS XE 17.1.1 Cisco IOS XE 16.12.1 Cisco IOS XE 16.9.1 Cisco IOS XE 16.6.2	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.1	√	√	√	√	√	√	√	√

[1] Validated OS is the version tested for compatibility and stability.

[2] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

[3] Minimum OS is the version in which the features got introduced.

[4] The IOS 12.x version does not fully support the Posture and Guest flows because of CSCsx97093. As a workaround, when you configure URL redirect in Cisco ISE, assign a value to “coa-skip-logical-profile.”

Network Access Control Capabilities of Cisco Wireless LAN Controllers

Table 2: Network Access Control Capabilities of Cisco Wireless LAN Controllers

Device	Validated OS [5]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [6]
WLC 2100	AireOS 7.0.252.0	!	√	*X*	!	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0 (minimum)	!	√	*X*	!	*X*	*X*	*X*	*X*

Device	Validated OS [5]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [6]
WLC 2504	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
WLC 3504	AirOS 8.5.105.0	√	√	√	√	√	√	√	Not validated
WLC 4400	AireOS 7.0.252.0	!	√	*X*	!	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0 (minimum)	!	√	*X*	!	*X*	*X*	*X*	*X*
WLC 2500	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AireOS 7.2.103.0 (minimum)	!	√	√	√	*X*	√	√	*X*
WLC 5508	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.114.x	√	√	√	√	*X*	√	√	√
	AireOS 8.3.140.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AireOS 7.0.116.0 (minimum)	!	√	*X*	!	*X*	*X*	*X*	√
WLC 5520	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AireOS 8.5.1.x	√	√	√	√	√	√	√	√
	AireOS 8.6.1.x	√	√	√	√	√	√	√	√
	AirOS 8.6.101.0(ED)	√	√	√	√	√	√	√	√
	AireOS 8.1.122.0 (minimum)	√	√	√	√	*X*	√	√	√

Device	**Validated OS** [5]	**AAA**	**Profiling**	**BYOD**	**Guest**	**Guest Originating URL**	**Posture**	**MDM**	**TrustSec** [6]
WLC 7500	AireOS 8.0.140.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.2.121.0	√	√	√	√	*X*	√	√	√
	AireOS 8.2.154.x	√	√	√	√	*X*	√	√	√
	AireOS 8.3.102.0	√	√	√	√	*X*	√	√	√
	AireOS 8.4.100.0	√	√	√	√	*X*	√	√	√
	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
	AireOS 7.2.103.0 (minimum)	**!**	√	*X*	*X*	*X*	*X*	*X*	*X*
WLC 8540	AireOS 8.1.131.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.1.122.0 (minimum)	√	√	√	√	*X*	√	√	*X*
WiSM1 6500	AireOS 7.0.252.0	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0 (minimum)	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
WiSM2 6500	AireOS 8.0.135.0	√	√	√	√	*X*	√	√	√
	AireOS 7.2.103.0 (minimum)	**!**	√	√	√	*X*	√	√	√
WLC 5760	IOS XE 3.6.4	√	√	√	√	√	√	√	√
	IOS XE 3.3 (minimum)	√	√	√	√	*X*	√	√	√

Device	Validated OS [5]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [6]
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1 Cisco IOS XE 17.9.1 Cisco IOS XE 17.6.1 Cisco IOS XE 17.5.1 Cisco IOS XE 17.4.1 Cisco IOS XE 17.3.1 Cisco IOS XE 17.2.1 Cisco IOS XE 17.1.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.10.1	√	√	√	√	√	√	√	√
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	AireOS 7.0.116.0	!	√	*X*	!	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0 (minimum)	!	√	*X*	!	*X*	*X*	*X*	*X*
Embedded Wireless Controller on Catalyst Access Points: Catalyst 9130 Series Catalyst 9120 Series Catalyst 9117 Series Catalyst 9115 Series Catalyst 9105 Series	Cisco IOS XE 17.6.1 Cisco IOS XE 17.5.1 Cisco IOS XE 17.4.1 Cisco IOS XE 17.3.1 Cisco IOS XE 17.2.1 Cisco IOS XE 17.1.1	√	√	√	√	√	√	√	*X*
	IOS XE 16.12.1	√	√	√	√	√	√	√	*X*

[5] Validated OS is the version tested for compatibility and stability.
[6] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

Refer to the Cisco Wireless Solutions Software Compatibility Matrix for a complete list of supported operating systems.

Note Due to CSCvi10594, IPv6 RADIUS CoA fails in AireOS Release 8.1 and later. As a workaround, you can use IPv4 RADIUS or downgrade Cisco Wireless LAN Controller to AireOS Release 8.0.

Note Cisco Wireless LAN Controllers (WLCs) and Wireless Service Modules (WiSMs) do not support downloadable ACLs (dACLs), but support named ACLs. Autonomous AP deployments do not support endpoint posturing. Profiling services are supported for 802.1X-authenticated WLANs starting from WLC release 7.0.116.0 and for MAB-authenticated WLANs starting from WLC 7.2.110.0. FlexConnect, previously known as Hybrid Remote Edge Access Point (HREAP) mode, is supported with central authentication configuration deployment starting from WLC 7.2.110.0. For additional details regarding FlexConnect support, refer to the release notes for the applicable wireless controller platform.

Network Access Control Capabilities of Cisco Access Points

Table 3: Network Access Control Capabilities of Cisco Access Points

Cisco Access Point	Minimum Cisco Mobility Express Version	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec
Cisco Aironet 1540 Series	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1560 Series	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1815i	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1815m	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 1815w	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X
Cisco Aironet 2800 Series	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X

Cisco Access Point	Minimum Cisco Mobility Express Version	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec
Cisco Aironet 3800 Series	Cisco Mobility Express 8.7.106.0	√	X	√	√	X	X	X	X

Network Access Control Capabilities of Cisco Routers

Table 4: Network Access Control Capabilities of Cisco Routers

Device	Validated OS [7] Minimum OS [8]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [9]
ISR 88x, 89x Series	IOS 15.3.2T(ED)	√	X	X	X	X	X	X
	IOS 15.2(2)T	√	X	X	X	X	X	X
ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X	IOS XE 17.1.1 IOS XE 17.2.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
ISR 19x, 29x, 39x Series	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.2(2)T	√	!	X	!	X	X	√
CE 9331	IOS XE 17.1.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√

Device	Validated OS [7] Minimum OS [8]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [9]
C8300-1N1S-4T2X C8300-1N1S-6T C8300-2N2S-4T2X C8300-2N2S-6T C8500-12X C8500-12X4QC C8200-1N-4T ISR1100-4G C8500L-8S4G	Cisco IOS XE 17.14.1 Cisco IOS XE 17.13.1 Cisco IOS XE 17.12.1 Cisco IOS XE 17.11.1 Cisco IOS XE 17.10.1 Cisco IOS XE 17.9.1 Cisco IOS XE 17.6.1 Cisco IOS XE 17.5.1 Cisco IOS XE 17.4.1	√	X	X	X	X	X	√
	Cisco IOS XE 17.4.1	√	X	X	X	X	X	√
CGR 2010	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
	IOS 15.3.2T(ED)	√	!	X	!	X	X	√
4451-XSM-X L2/L3 Ethermodule	IOS XE 3.11	√	√	√	√	√	√	√
	IOS XE 3.11	√	√	√	√	√	√	√

[7] Validated OS is the version tested for compatibility and stability.

[8] Minimum OS is the version in which the features got introduced.

[9] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

Note For CoA to function properly, the minimum IOS version required for Cisco ISR series to work with SM-X-40G8M2X and SM-X-16G4M2X modules is IOS XE 17.4.1.

Network Access Control Capabilities of Cisco Remote Access Platforms

Table 5: Network Access Control Capabilities of Cisco Remote Access Platforms

Device	Validated OS [10]	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec [11]
	Minimum OS [12]							
ASA 5500, ASA 5500-X (Remote Access Only)	ASA 9.2.1	NA	NA	√	NA	√	X	√
	ASA 9.1.5	NA	NA	X	NA	X	X	X

[10] Validated OS is the version tested for compatibility and stability.

[11] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.

[12] Minimum OS is the version in which the features got introduced.

Validated Cisco Meraki Devices

Table 6: Cisco Meraki Access Control Capabilities with ISE

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
Wireless								
MR20, MR70, MR28, MR78	√	√	√	√	X	√	√	X
MR30H, MR36, MR42/E, MR44, MR45, MR46/E, MR52, MR53E, MR56, MR74, MR76, MR86	√	√	√	√	√	√	√	X
Teleworker								
Z3/C	√	√	X	X	√ Transport MX18.1+	X	X	X

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
Switching								
MS120, MS125	√	√	√	*X*	*X*	*X*	√	CDP+LLDP
MS210, MS225, MS250	√	√	√	√	*X*	√	√	CDP+LLDP
MS350, MS355	√	√	√	√	*X*	√	√	CDP+LLDP
MS390	√	√	√	√	√	√	√	Full Device Sensor CDP/LLDP/DHCP/HTTP
MS410, MS425, MS450 (aggregation)	√	√	√	√	*X*	√	√	CDP+LLDP
Security and SD-WAN								
MX64/W, MX67/C/W, MX68/CW/W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450	√ 802.1X or MAB	√ 802.1X or MAB	*X*	*X*	√ Transport MX18.1+	*X*	*X*	*X*

Additional References

The following link contains additional resources that you can use when working with Cisco ISE: https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone 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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.