Cisco Identity Services Engine을 사용하는 네트워크 디바이스의 네트워크 액세스 제어 기능

Revised: 2022년 11월 2일

개요

Cisco ISE는 RADIUS, 관련 RFC 표준 및 TACACS+와 같은 프로토콜 표준을 지원합니다. 자세한 내용은 ISE 커뮤니티 리소스를 참조하십시오.

Cisco ISE는 표준 프로토콜을 준수하는 서드파티 RADIUS 디바이스와 완전하게 상호운용됩니다. RADIUS 기능의 지원 여부는 디바이스별 구현에 따라 달라집니다.

Cisco ISE는 준거 프로토콜을 준수하는 서드파티 TACACS+ 클라이언트 기기와 완전하게 상호운용됩니다. TACACS+ 기능의 지원 여부는 디바이스별 구현에 따라 달라집니다.

참고 이 문서에는 Cisco ISE에서 검증된 디바이스 목록만을 표시합니다. 따라서 이는 Cisco ISE에서 지원되는 디바이스의 전체 목록이 아닙니다.

이 문서에서는 디바이스 지원을 나타내는 데 다음과 같은 표기법이 사용됩니다.

- √: 완전히 지원
- X: 지원되지 않음
- ! : 제한적인 지원, 일부 기능은 지원되지 않음

Cisco 스위치의 NAC(Network Access Control) 기능

표 *1: Cisco* 스위치의 *NAC(Network Access Control)* 기능

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
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 17.9.1	√	√	√	√	√	√	√	√
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	√	√	√	√	√	√	√	√

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IR1101-K9	Cisco IOS XE 17.9.1	√	검증되지 않음	검증되지 않음	검증되지 않음	검증되지 않음	검증되지 않음	검증되지 않음	√
CGS 2520	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
Catalyst 1000	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	√
Catalyst 2960 LAN Base	Cisco IOS 15.0(2)SE11	√	√	√	√	*X*	√	√	*X*
	Cisco IOS v12.2(55) SE5 [4]	√	√	√	!	*X*	!	!	*X*
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	√	√	√	√	√	√	√	√

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
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	√	√	√	√	√	√	√	√
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	√	√	√	√	√	√	√	√

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
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	√	√	√	√	√	√	√	√
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*	√	√	√

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
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*	√	√	√
Catalyst 6500-E (Supervisor 720)	Cisco IOS 15.1(2)SY7	√	√	√	√	*X*	√	√	√
	Cisco IOS v12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (VSS2T40G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6807-XL Catalyst 6807-XL (VSS2T40G)	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*	√	√	√

디바이스	검증된 **OS** [1] 최소 **OS** [3]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [2]
다음을 포함한 Cisco Catalyst 9000 시리즈 스위치 제품군: Catalyst 9200 Catalyst 9300 Catalyst 9400 Catalyst 9500 Catalyst 9600	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] 검증된 OS는 호환성 및 안정성이 테스트된 버전입니다.
[2] Cisco TrustSec 기능 지원의 전체 목록은 Cisco TrustSec 제품 게시판을 참조하십시오.
[3] 최소 OS는 기능이 처음 도입된 버전입니다.
[4] IOS 12.x 버전은 CSCsx97093 때문에 포스처 및 게스트 플로우를 완전히 지원하지 않습니다. 이를 해결하려면 Cisco ISE에서 URL 리디렉션을 구성할 때 "coa-skip-logical-profile"에 값을 할당합니다.

Cisco Wireless LAN Controller의 네트워크 액세스 제어 기능

표 ***2: Cisco Wireless LAN Controller***의 네트워크 액세스 제어 기능

디바이스	검증된 **OS** [5]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [6]
WLC 2100	AireOS 7.0.252.0	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0(최소)	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
WLC 2504	AirOS 8.5.120.0(ED)	√	√	√	√	√	√	√	√
WLC 3504	AirOS 8.5.105.0	√	√	√	√	√	√	√	검증되지 않음

디바이스	검증된 **OS** [5]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [6]
WLC 4400	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0(최소)	!	√	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(최소)	!	√	√	√	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(최소)	!	√	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(최소)	√	√	√	√	X	√	√	√

디바이스	검증된 **OS** [5]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(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(최소)	**!**	√	*X*	*X*	*X*	*X*	*X*	*X*
WLC 8510	AireOS 8.0.135.0	√	√	√	√	*X*	√	√	*X*
	AireOS 7.4.121.0(최소)	√	√	*X*	*X*	*X*	*X*	√	*X*
WLC 8540	AireOS 8.1.131.0	√	√	√	√	*X*	√	√	*X*
	AireOS 8.1.122.0(최소)	√	√	√	√	*X*	√	√	*X*
WiSM1 6500	AireOS 7.0.252.0	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0(최소)	**!**	√	*X*	**!**	*X*	*X*	*X*	*X*
WiSM2 6500	AireOS 8.0.135.0	√	√	√	√	*X*	√	√	√
	AireOS 7.2.103.0(최소)	**!**	√	√	√	*X*	√	√	√
WLC 5760	IOS XE 3.6.4	√	√	√	√	√	√	√	√
	IOS XE 3.3(최소)	√	√	√	√	*X*	√	√	√
Catalyst 9800-80 Catalyst 9800-40 Catalyst 9800-L Catalyst 9800-CL	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	√	√	√	√	√	√	√	√

디바이스	검증된 **OS** [5]	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)** [6]
ISR용 WLC(ISR2 ISM, SRE700 및 SRE900)	AirOS 7.0.116.0	!	√	*X*	!	*X*	*X*	*X*	*X*
	AireOS 7.0.116.0(최소)	!	√	*X*	!	*X*	*X*	*X*	*X*
Catalyst Access Point의 내장 무선 컨트롤러: 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] 검증된 OS는 호환성 및 안정성이 테스트된 버전입니다.
[6] Cisco TrustSec 기능 지원의 전체 목록은 Cisco TrustSec 제품 게시판을 참조하십시오.

지원되는 운영체제의 전체 목록은 Cisco Wireless 솔루션 소프트웨어 호환성 매트릭스를 참조하십시오.

참고 CSCvi10594로 인해 IPv6 RADIUS CoA가 AireOS 릴리스 8.1 이상에서 실패합니다. 이 문제를 해결하기 위해 IPv4 RADIUS를 사용하거나 Cisco Wireless LAN 컨트롤러를 AireOS 릴리스 8.0으로 다운그레이드할 수 있습니다.

참고 Cisco WLCs(Wireless LAN Controllers) 및 WiSMs(Wireless Service Modules)는 dACLs(downloadable ACLs)를 지원하지 않지만 명명된 ACL은 지원합니다. 자동 AP 구축은 엔드포인트 보안 상태를 지원하지 않습니다. 프로파일링 서비스는 WLC 릴리스 7.0.116.0 이상의 802.1X 인증 WLAN 및 WLC 7.2.110.0 이상의 MAB 인증 WLAN을 지원합니다. FlexConnect(이전 명칭: HREAP(Hybrid Remote Edge Access Point) 모드)는 WLC 7.2.110.0 이상의 중앙 인증 구성 구축에 지원됩니다. FlexConnect 지원에 관한 자세한 내용은 해당 무선 컨트롤러 플랫폼의 릴리스 노트를 참조하십시오.

Cisco 액세스 포인트의 네트워크 액세스 제어 기능

표 ***3: Cisco*** 액세스 포인트의 네트워크 액세스 제어 기능

Cisco Access Point	최소 **Cisco Mobility Express** 버전	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**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 Aironet 3800 Series	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*

Cisco 라우터의 NAC(Network Access Control) 기능

표 *4: Cisco* 라우터의 *NAC(Network Access Control)* 기능

디바이스	검증된 **OS** [7] 최소 **OS** [8]	**AAA**	프로파일링	**BYOD**	**Guest**	보안 상태	**MDM**	트러스트섹**(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*	√
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 17.9.1 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] 검증된 OS는 호환성 및 안정성이 테스트된 버전입니다.
[8] 최소 OS는 기능이 처음 도입된 버전입니다.

[9] Cisco TrustSec 기능 지원의 전체 목록은 Cisco TrustSec 제품 게시판을 참조하십시오.

참고 CoA가 제대로 작동하려면 Cisco ISR 시리즈가 SM-X-40G8M2X 및 SM-X-16G4M2X 모듈과 함께 작동하는 데 필요한 최소 IOS 버전은 IOS XE 17.4.1입니다.

Cisco Remote Access 플랫폼의 NAC(Network Access Control) 기능

표 *5: Cisco Remote Access* 플랫폼의 *NAC(Network Access Control)* 기능

디바이스	검증된 **OS** [10] 최소 **OS** [12]	**AAA**	프로파일링	**BYOD**	**Guest**	보안 상태	**MDM**	트러스트섹**(TrustSec)** [11]
ASA 5500, ASA 5500-X(Remote Access만 해당)	ASA 9.2.1	해당 없음	해당 없음	√	해당 없음	√	*X*	√
	ASA 9.1.5	해당 없음	해당 없음	*X*	해당 없음	*X*	*X*	*X*

[10] 검증된 OS는 호환성 및 안정성이 테스트된 버전입니다.
[11] Cisco TrustSec 기능 지원의 전체 목록은 Cisco TrustSec 제품 게시판을 참조하십시오.
[12] 최소 OS는 기능이 처음 도입된 버전입니다.

검증된 Cisco Meraki 디바이스

디바이스	검증된 **OS** 최소 **OS**	**AAA**	프로파일링	**BYOD**	**Guest**	게스트 원래 **URL**	보안 상태	**MDM**	트러스트섹 **(TrustSec)**[13]
Meraki MS390	최신 MS 14.x 릴리스	!	√	*X*	*X*	*X*	*X*	*X*	√
	MS 14.5	!	√	*X*	*X*	*X*	*X*	*X*	√
Meraki MS120/MS125	최신 MS 14.x 릴리스	!	√	√	√	*X*	√	√	*X*
	MS 12.x	!	√	√	√	*X*	√	√	*X*
기타 모든 Meraki MS 모델	최신 MS 14.x 릴리스	√	√	√	√	*X*	√	√	*X*
	MS 12.0	!¹⁴	√	√	√	*X*	√	√	*X*

디바이스	검증된 OS 최소 OS	AAA	프로파일링	BYOD	Guest	게스트 원래 URL	보안 상태	MDM	트러스트섹(TrustSec)[13]
Meraki MR 802.1ac 웨이브 2 액세스 포인트	최신 MR 27.x 릴리스	√	√	√	√	√	√	√	√
	MR 26.0	√	√	√	√	√	√	√	X
Meraki MX 플랫폼	최신 버전	√	√	√	√	√	√	√	X
	최신 버전	√	√	√	√	√	√	√	X

[13] 트러스트섹(TrustSec)은 적응형 정책 기능을 사용하여 구현됩니다. 적응형 정책은 정적 및 동적 SGT 할당, 인라인 SGT 전파 및 SGT 기반 정책 시행을 지원합니다. 자세한 내용은 적응형 정책 개요를 참조하십시오.

[14] MS 14.5 이전 버전의 OS를 실행하는 Meraki MS 스위치는 그룹 정책 ACL 기능을 지원하지 않습니다. 자세한 내용은 Meraki MS 그룹 정책 액세스 제어 목록을 참조하십시오.

추가 참조 자료

다음 링크에는 Cisco ISE와 함께 작업할 때 사용할 수 있는 추가 리소스가 포함되어 있습니다.
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

통신, 서비스 및 추가 정보

- Cisco에서 시기에 맞는 관련된 정보를 받으려면 Cisco Profile Manager에 로그인합니다.
- 중요한 기술로 원하는 비즈니스 결과를 얻으려면 Cisco Services를 참조하십시오.
- 서비스 요청을 제출하려면 Cisco 지원을 참조하십시오.
- 안전하고 검증된 엔터프라이즈급 앱, 제품, 솔루션 및 서비스를 검색하고 찾아보려면 Cisco DevNet을 참조하십시오.
- 일반 네트워킹, 교육 및 인증서 제목을 얻으려면 Cisco Press를 참조하십시오.
- 특정 제품 또는 제품군에 대한 보증 정보를 찾으려면 Cisco Warranty Finder에 액세스합니다.

Cisco Bug Search Tool

Cisco BST(Bug Search Tool)는 Cisco 제품 및 소프트웨어에 있는 결함 및 취약점의 종합적인 목록을 유지관리하는 Cisco 버그 추적 시스템에 대한 게이트웨이입니다. BST에서는 제품 및 소프트웨어에 대한 자세한 결함 정보를 제공합니다.

문서 피드백

Cisco 기술 문서에 대한 피드백을 제공하려면 모든 온라인 문서의 오른쪽 창에 있는 피드백 양식을 사용하십시오.

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.