Cisco ISE(Identity Services Engine) 네트워크 구성 요소 호환성, 릴리스 3.1

개요 2

검증된 보안 제품 통합(pxGrid 사용) 23

검증된 Cisco Digital Network Architecture Center 릴리스 24

검증된 Cisco Prime Infrastructure 릴리스 24

검증된 Cisco Firepower Management Center 릴리스 24

검증된 Cisco Stealthwatch Management 릴리스 24

검증된 Cisco WAN 서비스 관리자 릴리스 25

위협 중심 NAC 지원 25

추가 참조 자료 25

통신, 서비스 및 추가 정보 25

Revised: 2022년 9월 30일

개요

참고 이 제품에 대한 문서 세트는 편견 없는 언어를 사용하기 위해 노력합니다. 이 설명서 세트의 목적상, 편향이 없는 언어는 나이, 장애, 성별, 인종 정체성, 민족 정체성, 성적 지향성, 사회 경제적 지위 및 교차성에 기초한 차별을 의미하지 않는 언어로 정의됩니다. 제품 소프트웨어의 사용자 인터페이스에서 하드코딩된 언어, RFP 설명서에 기초한 언어 또는 참조된 서드파티 제품에서 사용하는 언어로 인해 설명서에 예외가 있을 수 있습니다.

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

Cisco ISE는 표준 기반 인증을 위한 일반적인 RADIUS 동작을 구현하는 Cisco 또는 Cisco 이외 RADIUS 클라이언트 NAD(Network Access Device)와의 상호운용성을 지원합니다.

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

RADIUS

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

포스처 평가, 프로파일링, 웹 인증 등을 포함하는 일부 고급 활용 사례는 Cisco 이외의 디바이스에서 일관되게 사용할 수 없거나 제한적인 기능만 제공될 수 있습니다. 특정 소프트웨어 릴리스의 하드웨어 기능 또는 버그에 대해 모든 네트워크 디바이스 및 해당 소프트웨어를 검증하는 것이 좋습니다.

네트워크 디바이스가 동적 및 정적 URL 리디렉션을 모두 지원하지 않는 경우 Cisco ISE는 URL 리디렉션을 시뮬레이션하는 인증 VLAN 구성을 제공합니다. 자세한 내용은 Cisco ISE(Identity Services Engine) 관리자 가이드의 '보안 유선 액세스' 장의 'Cisco ISE의 서드파티 네트워크 디바이스 지원' 섹션을 참조하십시오.

TACACS+

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

네트워크 스위치에서 Cisco ISE의 특정 기능을 활성화하는 방법에 대한 자세한 내용은 Cisco Identity Services Engine 관리 가이드의 "Cisco ISE 기능 지원에 필요한 스위치 및 무선 LAN 컨트롤러 구성" 장을 참조하십시오.

ISE 커뮤니티 리소스

ISE가 내 네트워크 액세스 디바이스를 지원합니까?

타사 NAD 프로파일에 자세한 내용은 ISE 타사 NAD 프로파일 및 컨피그레이션을 참조하십시오.

Nexus 디바이스용 TACACS+를 구성하는 방법에 대한 자세한 내용은 Cisco ISE 디바이스 관리 규범 구축 가이드를 참조하십시오.

참고

- 일부 스위치 모델과 IOS 버전의 경우 단종되어 Cisco TAC에서 상호운용성이 지원되지 않을 수 있습니다.
- Cisco ISE 프로파일링 서비스에는 최신 버전의 NetFlow를 사용해야 합니다. NetFlow 5 버전을 사용하는 경우, 액세스 레이어의 기본 NAD에서만 사용할 수 있습니다.

Wireless LAN Controller의 경우 다음 사항에 유의하십시오.

- MAB(MAC Authentication Bypass)에서는 RADIUS 조회 기능으로 MAC 필터링을 지원합니다.
- MAC 필터링 기능과 함께 세션 ID와 COA를 지원하면 MAB 기능과 유사한 효과를 얻을 수 있습니다.
- DNS 기반 ACL 기능은 WLC 8.0 이상에서 지원됩니다. DNS 기반 ACL은 일부 액세스 포인트에서만 지원됩니다. 자세한 내용은 *Cisco* 액세스 포인트 릴리즈 노트를 참조하십시오.

Cisco ISE로 검증된 디바이스에 대한 자세한 내용은 Cisco Identity Services Engine으로 검증된 네트워크 디바이스 기능을 참조하십시오.

지원되는 프로토콜 표준, RFC 및 IETF 초안

Cisco ISE는 다음 프로토콜 표준, RFC(Requests for Comments) 및 IETF 초안을 준수합니다.

- 지원되는 **IEEE** 표준
  - IEEE802.1X-Std-2001
  - IEEE802.1X-Std-2004
- 지원되는 **IETF RFC**
  - RFC2138 - RADIUS
  - RFC2246 - TLSv1.0
  - RFC 2548 - Microsoft 벤더별 RADIUS 속성
  - RFC2759 - Microsoft PPP CHAP 확장, 버전 2
  - RFC2865 - RADIUS
  - RFC2866 - RADIUS 계정 관리
  - RFC2867 - 터널 프로토콜 지원을 위한 RADIUS 계정 관리 수정 사항
  - RFC2868 - 터널 프로토콜 지원을 위한 RADIUS 속성
  - RFC2869 - RADIUS 확장
  - RFC3579 - RADIUS EAP용 지원
  - RFC3580 - IEEE 802.1X RADIUS 사용 가이드라인
  - RFC3748 - EAP

- RFC4017 - 무선 LAN에 대한 EAP 방법 요구 사항
- RFC4851 - EAP-FAST
- RFC5176 - RADIUS에 대한 유동 권한 부여 확장
- RFC5216 - EAP-TLS 인증 프로토콜
- RFC5281 - Extensible Authentication Protocol Tunneled Transport Layer Security 인증 프로토콜 버전 0(EAP-TTLSv0)
- RFC5422 - EAP-FAST(Flexible Authentication via Secure Tunneling Extensible Authentication Protocol)를 사용하는 동적 프로비저닝
- RFC5425 - 시스템 로그에 대한 TLS(Transport Layer Security) 전송 매핑
- RFC6587 - TCP를 통한 시스템 로그 메시지 전송
- RFC7360 - RADIUS에 대한 전송 레이어로서의 DTLS(Datagram Transport Layer Security)

다음 RFC는 부분적으로 지원됩니다.

- RFC 2548 - Microsoft 벤더별 RADIUS 속성
- RFC2882 - 네트워크 액세스 서버 요구 사항: 확장 RADIUS 사례
- RFC7030 - EST(Enrollment over Secure Transport)(BYOD 플로우의 일부로 지원됨)
- RFC7170 - TEAP(Tunnel Extensible Authentication Protocol) 버전 1

- 지원되는 **IETF** 초안
  - IETF 초안 - PEAP 버전 0
  - IETF 초안 - PEAP 버전 1
  - IETF 초안 - PEAP 버전 2
  - IETF 초안 - Microsoft EAP CHAP 확장 버전 2

RADIUS 프록시 서비스를 위한 **AAA** 속성

RADIUS 프록시 서비스를 사용하려면 RADIUS 통신에 다음과 같은 AAA(인증, 권한 부여 및 계정 관리) 속성이 포함되어야 합니다.

- Calling-Station-ID(IP 또는 MAC_ADDRESS)
- RADIUS::NAS_IP_Address
- RADIUS::NAS_Identifier

서드파티 VPN 집중기를 위한 AAA 속성

Cisco ISE와 VPN 집중기를 통합하는 경우, RADIUS 통신에 다음과 같은 AAA(인증, 권한 부여 및 계정 관리) 속성이 포함되어야 합니다.

- Calling-Station-ID(MAC 또는 IP 주소별로 개별 클라이언트 추적)
- User-Name(로그인 이름으로 원격 클라이언트 추적)
- NAS-Port-Type(연결 유형을 VPN으로 확인하는 데 도움이 됨)
- RADIUS 계정 관리 시작(공식 세션 시작 트리거)
- RADIUS 계정 관리 중지(공식 세션 종료를 트리거하고 ISE 라이선스 릴리스)
- IP 주소 변경 시 RADIUS 계정 관리 임시 업데이트(예: 웹 기반에서 전체 터널 클라이언트로 SSL VPN 연결 전환)

참고 VPN 디바이스의 경우, 신뢰할 수 있는 네트워크에 있는 동안 엔드포인트를 추적하도록 클라이언트의 VPN 할당 IP 주소로 설정된 Framed-IP-Address 속성이 RADIUS 계정 관리 메시지에 포함되어야 합니다.

시스템 요구 사항

중단 없는 Cisco ISE 컨피그레이션의 경우, 다음 시스템 요구 사항이 충족되는지 확인합니다.

이 Cisco ISE 릴리스의 하드웨어 플랫폼 및 설치에 대한 자세한 내용은 *Cisco Identity Services Engine* 하드웨어 설치 설명서를 참조하십시오.

스마트 라이선싱을 지원하는 SSM On-Prem 서버 릴리스에 대한 자세한 내용은 해당 릴리스의 Cisco ISE 관리자 가이드에서 "라이선싱" 장에서 스마트 라이선싱을 위해 Smart Software Manager On-Prem 구성 항목을 참조하십시오.

지원되는 하드웨어

Cisco ISE, 릴리스 3.1은 다음 플랫폼에서 설치하고 실행할 수 있습니다.

표 *1:* 지원되는 플랫폼

하드웨어 플랫폼	컨피그레이션
Cisco SNS-3595-K9(대형)	어플라이언스 하드웨어 사양은 *Cisco SNS(Secure Network Server)* 어플라이언스 하드웨어 설치 설명서를 참조하십시오.
Cisco SNS-3615-K9(소형)	
Cisco SNS-3655-K9(중간)	
Cisco SNS-3695-K9(대형)	

설치 후에는 위 표에 나열된 플랫폼에서 Administration(관리), Monitoring(모니터링) 또는 pxGrid와 같은 특정 구성 요소 페르소나를 사용하여 Cisco ISE를 구성할 수 있습니다. 이러한 페르소나 외에, Cisco ISE에는 Policy Service(정책 서비스) 내의 다른 유형의 페르소나(예, Profiling Service(프로파일링 서비스), Session Services(세션 서비스), TC-NAC(Threat-Centric

NAC), TrustSec용 SXP 서비스, TACACS+ Device Admin Service(TACACS+ 디바이스 관리 서비스), Passive Identity Service(패시브 ID 서비스))가 포함되어 있습니다.

주의

- Cisco ISE 3.1 이상의 릴리스는 Cisco SNS(Secured Network Server) 3515 어플라이언스를 지원하지 않습니다.
- Cisco ISE, 릴리스 2.4 이상에서 Cisco SNS 3400 Series 어플라이언스가 지원되지 않습니다.
- VM 어플라이언스 컨피그레이션에는 16GB 미만의 메모리 할당이 지원되지 않습니다. Cisco ISE 동작 문제가 발생하는 경우, Cisco TAC(Technical Assistance Center)에서 케이스를 열기 전에 모든 사용자가 할당된 메모리를 16GB 이상으로 변경해야 합니다.
- Cisco ISE, 릴리스 2.0 이상에서는 레거시 ACS(Access Control Server) 및 NAC(Network Access Control) 어플라이언스(Cisco ISE 3300 Series 포함)가 지원되지 않습니다.

지원되는 가상 환경

Cisco ISE는 다음과 같은 가상 환경 플랫폼을 지원합니다.

- VMware ESXi 6.5 이상, 7.x
  - Cisco ISE는 VMware ESXi 6.5가 설치된 Cisco HyperFlex HX-Series에서 검증됨
  - VMware 클라우드에 Cisco ISE를 설치하는 프로세스는 VMware 가상 컴퓨터에 Cisco ISE를 설치하는 프로세스와 정확히 동일합니다.
    - AWS(Amazon Web Services)의 VMware Cloud에 구축된 Cisco ISE 가상 컴퓨터: Cisco Cloud가 AWS에서 제공하는 SDDC(Software Defined Data Center)에서 Cisco ISE를 호스팅할 수 있습니다. 온프레미스 구축, 필수 디바이스 및 서비스에 연결할 수 있도록, VMware Cloud에 적절한 보안 그룹 정책을 구성해야 합니다.
    - Azure VMware 솔루션에 구축된 Cisco ISE 가상 컴퓨터: Azure VMware 솔루션은 기본적으로 Cisco ISE를 VMware 가상 컴퓨터로 호스팅할 수 있는 Azure에서 VMware 워크로드를 실행합니다.

참고 Cisco ISE 3.1에서는 VMware 마이그레이션 기능을 사용하여 호스트 간에 가상 시스템(VM) 인스턴스(모든 페르소나 실행)를 마이그레이션할 수 있습니다. Cisco ISE는 핫 마이그레이션과 콜드 마이그레이션을 모두 지원합니다. 핫 마이그레이션은 실시간 마이그레이션 또는 vMotion이라고도 합니다. 핫 마이그레이션 중에는 Cisco ISE를 종료하거나 전원을 끌 필요가 없습니다. Cisco ISE VM의 가용성을 중단하지 않고 마이그레이션할 수 있습니다.

- Microsoft Windows Server 2012 R2 이상의 Microsoft Hyper-V
- QEMU 2.12.0-99상의 KVM
- Nutanix AHV 20201105.2096

가상 머신 요구 사항에 대한 자세한 내용은 사용 중인 Cisco ISE 버전의 *Cisco Identity Services Engine* 설치 설명서를 참조하십시오.

FIPS(연방 정보 처리 표준) 모드 지원

Cisco ISE는 임베디드 FIPS(연방 정보 처리 표준) 140-2 검증 암호화 모듈, Cisco FIPS Object Module 7.2 버전(인증서 #3790)을 사용합니다. FIPS 컴플라이언스 클레임에 대한 자세한 내용은 글로벌 정부 인증을 참조하십시오.

Cisco ISE에서 FIPS 모드가 활성화된 경우, 다음 사항을 고려하십시오.

- 모든 비FIPS 호환 암호 그룹은 비활성화됩니다.
- 인증서 및 개인 키는 FIPS 호환 해시 및 암호화 알고리즘만 사용해야 합니다.
- RSA 개인 키는 2,048비트 이상이어야 합니다.
- ECDSA(Elliptical Curve Digital Signature Algorithm) 개인 키는 224비트 이상이어야 합니다.
- DHE(Diffie-Hellman Ephemeral) 암호는 2,048비트 이상의 DH(Diffie-Hellman) 매개변수와 함께 작동합니다.
- SHA1은 ISE 로컬 서버 인증서를 생성할 수 없습니다.
- EAP-FAST의 익명 PAC 프로비저닝 옵션이 비활성화되었습니다.
- 로컬 SSH 서버는 FIPS 모드에서 작동합니다.
- 다음 프로토콜은 RADIUS에 대한 FIPS 모드에서 지원되지 않습니다.
    - EAP-MD5
    - PAP
    - CHAP
    - MS-CHAPv1
    - MS-CHAPv2
    - LEAP

검증된 브라우저

Cisco ISE 3.1는 다음 브라우저에서 검증되었습니다.

- Mozilla Firefox 82부터 102 이하 버전
- Mozilla Firefox ESR 91.3 이하 버전
- Google Chrome 86부터 103 이하 버전
- Microsoft Edge, 최신 버전 및 최신 버전보다 이전 버전

확인된 External Identity Sources(외부 ID 소스)

참고 지원되는 Active Directory 버전은 Cisco ISE 및 Cisco ISE-PIC에서 동일합니다.

표 2: 확인된 External Identity Sources(외부 ID 소스)

External Identity Source(외부 ID 소스)	버전
Active Directory [1]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [2]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [3]	Windows Server 2019
LDAP 서버	
SunONE LDAP Directory Server	버전 5.2
OpenLDAP Directory Server	버전 2.4.23
모든 LDAP v3 호환 서버	LDAP v3와 호환되는 모든 버전
토큰 서버	
RSA ACE/Server	6.x Series
RSA 인증 관리자	7.x 및 8.x Series
RADIUS RFC 2865와 호환되는 모든 토큰 서버	RFC 2865를 준수하는 모든 버전
SAML(Security Assertion Markup Language) SSO(Single Sign-On)	
Microsoft Azure	최신
OAM(Oracle Access Manager)	버전 11.1.2.2.0
OIF(Oracle Identity Federation)	버전 11.1.1.2.0
PingFederate 서버	버전 6.10.0.4
PingOne 클라우드	최신
보안 인증	8.1.1

External Identity Source(외부 ID 소스)	버전
모든 SAMLv2 호환 ID 제공자	SAMLv2를 준수하는 모든 ID 제공자 버전
ODBC(Open Database Connectivity) ID 소스	
Microsoft SQL Server	Microsoft SQL Server 2012
Oracle	Enterprise Edition 릴리스 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
소셜 로그인(게스트 사용자 계정용)	
Facebook	최신

[1] Cisco ISE에는 최대 200개의 도메인 컨트롤러만 추가할 수 있습니다. 제한을 초과하면 다음과 같은 오류가 표시됩니다.

```
Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200(<DC FQDN> 생성 오류 - DC 수가 허용된 최대 200개를 초과)
```

[2] Cisco ISE는 Microsoft Windows Active Directory 2012 R2의 모든 레거시 기능을 지원합니다. 그러나 Protective User Groups와 같은 Microsoft Windows Active Directory 2012 R2의 신기능은 지원하지 않습니다.

[3] Cisco ISE 2.6 패치 4 이상은 Microsoft Windows Active Directory 2019의 모든 레거시 기능을 지원합니다.

자세한 내용은 *Cisco ISE(Identity Services Engine) 관리자 설명서*를 참조하십시오.

지원되는 통합 엔드포인트 관리 및 모바일 디바이스 관리 서버

지원되는 MDM 서버에는 다음 벤더의 제품이 포함됩니다.

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco0 Meraki Systems Manager
- Citrix XenMobile 10.x(온프레미스)
- Globo
- IBM MaaS360
- Ivanti(이전 명칭 MobileIron UEM), 코어 및 클라우드 UEM 서비스

  Cisco ISE 3.1에서 랜덤 처리하고 MAC 주소를 변경하는 사용 사례의 경우 GUID 값을 수신하려면 MobileIron Core 11.3.0.0 Build 24 이상 릴리스를 통합해야 합니다.

참고 일부 MobileIron 버전은 Cisco ISE에서 작동하지 않습니다. MobileIron은 이 문제를 인식하고 수정했습니다. 자세한 내용은 MobileIron에 문의하십시오.

- JAMF Casper Suite
- Microsoft 엔드포인트 구성 관리자
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE(이전 명칭 AirWatch)
- 42 Gears

서버를 Cisco ISE와 통합하기 위해 엔드포인트 관리 서버에서 수행해야 하는 구성은 UEM 및 MDM 서버를 Cisco ISE와 통합을 참조하십시오.

ISE 커뮤니티 리소스

방법: Meraki EMM / MDM과 ISE 통합

지원되는 안티바이러스 및 안티멀웨어 제품

Cisco ISE 포스처 에이전트에서 지원하는 안티바이러스 및 악성코드 차단 제품에 대한 자세한 내용은 Cisco AnyConnect ISE 포스처 지원 차트를 참조하십시오.

지원되는 암호

Cisco ISE를 새로 설치하거나 새로 고칠 때, SHA1 암호는 기본적으로 비활성화되어 있습니다. 그러나 Cisco ISE의 기존 버전에서 업그레이드하는 경우, SHA1 암호는 이전 버전의 옵션을 유지합니다. **Allow SHA1 Ciphers(SHA1** 암호 허용**)** 필드 (**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**)를 사용하여 SHA1 암호 설정을 보고 변경할 수 있습니다

참고 이 사항은 Admin Portal(관리자 포털)에는 적용되지 않습니다. FIPS(연방 정보 처리 표준) 모드 에서 실행 중인 경우, 업그레이드 시 관리 포털에서 SHA1 암호가 제거되지 않습니다.

Cisco ISE는 TLS 버전 1.0, 1.1 및 1.2를 지원합니다.

Cisco ISE는 RSA 및 ECDSA 서버 인증서를 지원합니다. 다음 Elliptic Curve가 지원됩니다.

- secp256r1
- secp384r1
- secp521r1

참고 Cisco ISE는 현재 OpenJDK 1.8 구현의 제한 사항으로 인해 Elliptical Curve에 대해 SHA256withECDSA 서명 알고리즘이 있는 중간 인증서를 지원하지 않습니다.

다음 표에는 지원되는 암호 그룹이 나열되어 있습니다.

암호 그룹	**Cisco ISE**가 **EAP** 서버로 구성된 경우 **Cisco ISE**가 **RADIUS DTLS** 서버로 구성된 경우	**Cisco ISE**가 **HTTPS** 또는 보안 **LDAP** 서버에서 **CRL**을 다운로드하는 경우 **Cisco ISE**가 보안 시스템 로그 클라이언트 또는 보안 **LDAP** 클라이언트로 구성된 경우 **Cisco ISE**가 **CoA**의 **RADIUS DTLS** 클라이언트로 구성된 경우
TLS 1.0 지원	TLS 1.0이 허용되는 경우 (DTLS 서버는 DTLS 1.2만 지원) Cisco ISE 2.3 이상에서는 TLS 1.0 허용 옵션이 기본적으로 비활성화되어 있습니다. 이 옵션을 비활성화하면 TLS 기반 EAP 인증 방법(EAP-TLS, EAP-FAST/TLS) 및 802.1X supplicant에 대해 TLS 1.0이 지원되지 않습니다. TLS 1.0에서 TLS 기반 EAP 인증 방법을 사용하려면 **Security Settings(**보안 설정**)** 창에서 TLS 1.0 허용 확인란을 선택합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **Security Settings(**보안 설정**)**.	TLS 1.0이 허용되는 경우 (DTLS 클라이언트는 DTLS 1.2만 지원)
TLS 1.1 지원	TLS 1.1이 허용되는 경우	TLS 1.1이 허용되는 경우
ECC DSA 암호		
ECDHE-ECDSA-AES256-GCM-SHA384	예	예
ECDHE-ECDSA-AES128-GCM-SHA256	예	예
ECDHE-ECDSA-AES256-SHA384	예	예

ECDHE-ECDSA-AES128-SHA256	예	예
ECDHE-ECDSA-AES256-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
ECDHE-ECDSA-AES128-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
ECC RSA 암호		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES256-SHA384	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES128-SHA256	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1이 허용되는 경우	ECDHE-RSA/SHA-1이 허용되는 경우
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1이 허용되는 경우	ECDHE-RSA/SHA-1이 허용되는 경우
DHE RSA 암호		
DHE-RSA-AES256-SHA256	아니요	예
DHE-RSA-AES128-SHA256	아니요	예
DHE-RSA-AES256-SHA	아니요	SHA-1이 허용되는 경우
DHE-RSA-AES128-SHA	아니요	SHA-1이 허용되는 경우
RSA 암호		
AES256-SHA256	예	예
AES128-SHA256	예	예
AES256-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
AES128-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
3DES 암호		
DES-CBC3-SHA	3DES/SHA-1이 허용되는 경우	3DES/DSS 및 SHA-1이 활성화된 경우
DSS 암호		
DHE-DSS-AES256-SHA	아니요	3DES/DSS 및 SHA-1이 활성화된 경우

DHE-DSS-AES128-SHA	아니요	3DES/DSS 및 SHA-1이 활성화된 경우
EDH-DSS-DES-CBC3-SHA	아니요	3DES/DSS 및 SHA-1이 활성화된 경우
약한 RC4 암호		
RC4-SHA	허용된 프로토콜 페이지에서 "약한 암호 허용" 옵션을 활성화하고 SHA-1이 허용되는 경우	아니요
RC4-MD5	허용된 프로토콜 페이지에서 "약한 암호 허용" 옵션을 활성화한 경우	아니요
EAP-FAST 익명 프로비저닝만 해당: ADH-AES-128-SHA	예	아니요
피어 인증서 제한 사항		
KeyUsage 검증	클라이언트 인증서에는 다음 암호에 대한 KeyUsage=Key Agreement 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다. • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

ExtendedKeyUsage 검증	클라이언트 인증서에는 다음 암호에 대한 KeyUsage=Key Encipherment 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다. • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	서버 인증서에는 ExtendedKeyUsage=Server Authentication이 있어야합니다.

검증된 **OpenSSL** 버전

Cisco ISE 3.1은 OpenSSL 1.1.1k로 검증되었습니다.

검증된 클라이언트 시스템 운영체제, **supplicant** 및 에이전트

이 섹션에는 각 클라이언트 시스템 유형의 검증된 클라이언트 시스템 운영체제, 브라우저 및 에이전트 버전이 나와 있습니다. 모든 디바이스의 웹 브라우저에서 쿠키가 활성화되어 있어야 합니다. Cisco AnyConnect-ISE 포스처 지원 차트는 https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html에서 제공됩니다.

다음 클라이언트 머신 유형은 BYOD(Bring Your Own Device) 및 Posture 워크플로우에 대해 검증되었습니다.

- Apple iOS
- Apple macOS
- Google Android
- Google Chromebook
- Linux
- Microsoft Windows

Cisco ISE, 릴리스 2.3 이상에서는 Cisco AnyConnect 및 Cisco Temporal Agent만 지원합니다.

모든 표준 802.1X supplicant는 Cisco ISE에 의해 지원되는 표준 인증 프로토콜을 지원하는 경우에 Cisco ISE 릴리스 2.4 이상의 표준 및 고급 기능과 함께 사용할 수 있습니다. VLAN 변경 인증 기능이 무선 구축 환경에서 작동하려면 서플리컨트가 VLAN 변경 시 IP 주소 갱신을 지원해야 합니다.

포스처 및 BYOD(Bring Your Own Device) 플로우는 최신 포스처 피드 업데이트를 기반으로 Cisco ISE UI에 나열된 운영체제의 공식 출시 릴리스에서 지원됩니다. 포스처 및 BYOD 플로우는 Cisco ISE UI에 나열된 베타 macOS 릴리스에서도 작동할 수 있습니다. 예를 들어 **macOS 12 Beta(all)(macOS 12** 베타**(**모두**))**가 Cisco ISE UI에 나열되어 있으면 포스처 및 BYOD 플로우가 macOS 12 베타 엔드포인트에서 작동할 수 있습니다. 베타 운영체제 릴리스는 초기 릴리스와 공식 출시 릴리스 사이에 상당한 변화를 겪기 때문에 가능한 최선의 방법으로 지원이 제공됩니다.

운영 체제(OS)를 새 버전으로 업데이트하는 경우 Posture Feed Server에서 업데이트된 OS 버전의 지원 및 반영에 몇 시간 또는 하루의 지연이 발생할 수 있습니다.

Apple iOS

이 클라이언트 머신 유형은 BYOD 및 포스처 워크플로에 대해 검증되었습니다.

Apple iOS 디바이스는 Cisco ISE 또는 802.1x에서 PEAP(Protected Extensible Authentication Protocol)를 사용하며, 공용 인증서에는 iOS 디바이스에서 네트워크 액세스를 사용하여 확인해야 하는 CRL 배포 지점이 포함되어 있습니다. 네트워크를 인증하려면 iOS 디바이스에서 "Confirm/Accept(확인/수락)"를 클릭하십시오.

다음과 같은 Apple iOS 버전이 Cisco ISE에서 검증되었습니다.

- Apple iOS 13.x
- Apple iOS 12.x
- Apple iOS 11.x

참고

- Apple iOS 12.2 이상 버전을 사용하는 경우 다운로드한 인증서/프로파일을 수동으로 설치해야 합니다. 이렇게 하려면 Apple iOS 디바이스에서 **Settings(**설정**) > General(**일반**) > Profile(**프로파일**)**을 선택하고 **Install(**설치**)**을 클릭합니다.
- Apple iOS 12.2 이상 버전을 사용하는 경우 RSA 키 크기는 2048비트 이상이어야 합니다. 그렇지 않으면 BYOD 프로파일을 설치하는 동안 오류가 표시될 수 있습니다.
- Apple iOS 13 이상 버전을 사용하는 경우, **SAN** 필드에서 **DNS Name(DNS** 이름**)**으로 **<<FQDN>>**을 추가하여 포털 역할에 대한 SSC(자가서명 인증서)를 다시 생성합니다.
- Apple iOS 13 이상 버전을 사용하는 경우 **SHA-256** 이상이 서명 알고리즘으로 선택되었는지 확인합니다.

Apple macOS

이 클라이언트 머신 유형은 BYOD 및 포스처 워크플로에 대해 검증되었습니다.

표 *3: Apple macOS*

클라이언트 시스템 운영 체제	**AnyConnect**
Apple macOS 12	4.10.04071 이상
Apple macOS 11	4.9.04043 이상
Apple macOS 10.15	4.8.01090 이상
Apple macOS 10.14	4.8.01090 이상
Apple macOS 10.13	4.8.01090 이상

Cisco ISE는 AnyConnect 4.x의 이전 릴리스에서 작동합니다. 그러나 최신 AnyConnect 릴리스에서만 최신 기능을 지원합니다.

참고 Apple macOS 11의 경우 Cisco AnyConnect 4.9.04043 이상 및 MAC OSX 컴플라이언스 모듈 4.3.1466.4353 이상을 사용해야 합니다.

Apple macOS 11을 사용하는 경우 Cisco Network Setup Assistant를 설치할 때 프로파일을 수동으로 설치하라는 메시지가 표시될 수 있습니다. 이 경우 다음을 수행해야 합니다.

1. Downloads 폴더로 이동합니다.
2. cisco802dot1xconfiguration.mobileconfig 파일을 더블 클릭합니다.
3. **System(**시스템**)** > **Preferences(**기본 설정**)**를 선택합니다.
4. **Profiles(**프로파일**)**를 클릭합니다.
5. 프로파일을 설치합니다.
6. Cisco Network Setup Assistant에 관련 메시지가 표시되면 **OK(**확인**)**를 클릭하여 설치를 진행합니다.

참고 MAC OSX 3.1.0.1 버전용 Supplicant Provisioning Wizard 번들은 모든 Cisco ISE 릴리스에서 공통적으로 사용됩니다. Cisco ISE 2.4 패치 12, Cisco ISE 2.6 패치 8, Cisco ISE 2.7 패치 3 및 Cisco ISE 3.0 패치 2에서 확인되었습니다.

Cisco ISE 포스처 에이전트에서 지원하는 Windows 및 MAC OSX 악성코드 차단, 패치 관리, 디스크 암호화 및 방화벽 제품에 대한 자세한 내용은 Cisco AnyConnect-ISE 포스처 지원 차트를 참조하십시오.

참고

- 모든 브라우저에서 보고되는 Apple macOS 버전이 10.15.7로 제한되고 사용자 프라이버시가 강화되었습니다.
- 프로비저닝 중에는 Apple macOS 11 엔드포인트를 식별할 수 없습니다. 이로 인해 클라이언트에서 Apple macOS 11을 실행 중인 경우 포스처 및 BYOD 플로우에서 CP 정책 일치에 문제가 발생합니다. 이 문제를 해결하려면 Apple macOS 11에 대한 포스처 및 BYOD 플로우를 모든 macOS로 CP 정책 매핑으로 진행합니다.
- 분류 중에는 Apple macOS 11 엔드포인트를 식별할 수 없습니다. 이로 인해 클라이언트에서 Apple macOS 11을 실행 중인 경우 프로파일링 정책 일치에 문제가 발생합니다.

Cisco ISE 릴리스 3.0부터는 지원되는 모든 Apple macOS 릴리스에서 Agentless Posture(에이전트리스 포스처) 기능을 사용할 수 있습니다. 사용 중인 Cisco ISE 릴리스의 *Cisco ISE* 관리자 가이드에서 '컴플라이언스' 장의 '에이전트리스 상태' 항목을 참조하십시오.

Google Android

이 클라이언트 머신 유형은 BYOD 및 포스처 워크플로에 대해 검증되었습니다.

특정 디바이스에서 안드로이드 구현 시 개방형 액세스가 가능하기 때문에 Cisco ISE는 특정 안드로이드 OS 버전 및 디바이스 조합을 지원하지 않을 수 있습니다.

다음과 같은 Google 안드로이드 버전이 Cisco ISE에서 검증되었습니다.

- Google Android 10.x
- Google 안드로이드 9.x
- Google 안드로이드 8.x
- Google 안드로이드 7.x

SPW(Supplicant Provisioning Wizard)를 시작하기 전에 안드로이드 9.x 및 10.x 디바이스에서 위치 서비스가 활성화되어 있는지 확인하십시오.

안드로이드는 더 이상 CN(Common Name)을 사용하지 않습니다. 호스트 이름이 SAN(subjectAltName) 확장명에 포함되어야 합니다. 그렇지 않으면 신뢰가 실패합니다.SSC(자가서명 인증서)를 사용하는 경우 포털의 SAN 드롭다운 목록에서 Domain Name(도메인 이름) 또는 IP Address(IP 주소) 옵션을 선택하여 Cisco ISE 자가서명 인증서를 다시 생성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

안드로이드 9.x를 사용하는 경우 안드로이드 9용 NSA를 가져오려면 Cisco ISE에서 포스처 피드를 업데이트해야 합니다.

Google Chromebook

이 클라이언트 머신 유형은 BYOD 및 포스처 워크플로에 대해 검증되었습니다.

Google Chromebook은 관리되는 디바이스이며 포스처 서비스를 지원하지 않습니다. 자세한 내용은 *Cisco Identity Services Engine* 관리 지침서를 참조하십시오.

표 *4: Google Chromebook*

클라이언트 시스템 운영 체제	웹 브라우저	**Cisco ISE**
Google Chromebook	Google Chrome 49 이상 버전	Cisco ISE 2.4 패치 8

URL이 성공적으로 리디렉션되더라도 Cisco ISE BYOD 또는 게스트 포털이 Chrome 운영체제 73에서 실행되지 않을 수 있습니다. Chrome 운영체제 73에서 포털을 실행하려면 아래 단계를 수행합니다.

1. Subject Alternative Name(주체 대체 이름) 필드를 입력해 ISE GUI에서 새 자체 서명 인증서를 생성합니다. DNS 및 IP 주소를 모두 입력해야 합니다.
2. 인증서를 최종 클라이언트(Chromebook)로 내보내고 복사합니다.
3. **Settings(**설정**) > Advanced(**고급**) > Privacy and Security(**개인 정보 및 보안**) > Manage certificates(**인증서 관리**) > Authorities(**권한 부여**)**를 선택합니다.
4. 인증서를 가져옵니다.
5. 브라우저를 닫고 포털 리디렉션을 시도합니다.

Chromebook 76 이상에서 EAP용 내부 CA를 사용하여 EAP-TLS 설정을 구성하는 경우 SAN 필드가 포함된 CA 인증서 체인을 Google Admin Console **Device Management(**디바이스 관리**) > Network(**네트워크**) > Certificates(**인증서**)**에 업로드합니다. CA 체인이 업로드되면 SAN 필드가 포함된 Cisco ISE 생성 인증서가 **Chromebook Authorities(Chromebook** 인증 기관**)** 섹션에 매핑되어 Cisco ISE 인증서가 신뢰할 수 있는 것으로 간주됩니다.

서드파티 CA를 사용하는 경우에는 CA 체인을 Google Admin Console로 가져올 필요가 없습니다. **Settings(**설정**) > Advanced(**고급**) > Privacy and Security(**개인 정보 및 보안**) > Manage certificates (**인증서 관리**) > Server certificate Authority(**서버 인증 기관**)**를 선택하고 드롭다운 목록에서 **Use any default Certificate Authority(**기본 인증 기관 사용**)**를 선택합니다.

Linux

이 클라이언트 머신 유형은 BYOD 및 포스처 워크플로에 대해 검증되었습니다.

표 *5: Linux*

클라이언트 시스템 운영 체제	**Cisco AnyConnect**
Red Hat Enterprise Linux(RHEL)	Cisco AnyConnect 릴리스 4.10 MR2[4.10.02086] 이상
RHEL 7.5, RHEL 7.9	
RHEL 8.x	
SUSE Linux Enterprise Server(SLES)	
SLES 12.3 이상	
SLES 15.x	
Ubuntu	
Ubuntu 18.04	
Ubuntu 20.04	

Microsoft Windows

표 *6: Microsoft Windows*

클라이언트 시스템 운영 체제	서플리컨트**(802.1X)**	**Cisco Temporal Agent**	**AnyConnect**[4]
Microsoft Windows 11			
• Windows 11 Enterprise • Windows 11 Professional • Windows 11 Education • Windows 11 Home	• Microsoft Windows 802.1x 클라이언트 • Cisco AnyConnect Network Access Manager	4.10.04065 이상	4.10.04065 이상
Microsoft Windows 10			

클라이언트 시스템 운영 체제	서플리컨트**(802.1X)**	**Cisco Temporal Agent**	**AnyConnect**[4]
• Windows 21H2 • Windows 21H1 • Windows 20H2 • Windows 20H1 • Windows 19H2 • Windows 19H1 • Windows 10 Enterprise • Windows 10 Enterprise N • Windows 10 Enterprise E • Windows 10 Enterprise LTSB • Windows 10 Enterprise N LTSB • Windows 10 Professional • Windows 10 Professional N • Windows 10 Professional E • Windows 10 Education • Windows 10 Home • Windows 10 Home 중국어 • Windows 10.0 SLP(Single Language Pack)	• Microsoft Windows 10 802.1X 클라이언트 • Cisco AnyConnect Network Access Manager	4.5 이상	4.8.01090 이상

[4] AnyConnect NAM(AnyConnect Network Access Manager)을 설치한 경우 NAM은 Windows 기본 supplicant를 802.1X supplicant로 우선 적용하며 BYOD 플로우를 지원하지 않습니다. NAM을 완전히 비활성화하거나 특정 인터페이스에서 비활성화해야 합니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리 지침서를 참조하십시오.

BYOD, 게스트 및 클라이언트 프로비저닝 포털에 대해 Firefox 70에서 무선 리디렉션을 활성화하려면 다음과 같이 합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**.
2. **Allow SHA1 ciphers(SHA1** 암호 허용**)** 체크 박스를 선택합니다. SHA1 암호는 기본적으로 비활성화되어 있습니다.

3. Firefox 브라우저에서 **Options(**옵션**)** > **Privacy & Settings(**개인 정보 및 설정**)** > **View Certificates(**인증서 보기**)** > **Servers(**서버**)** > **Add Exception(**예외 추가**)**을 선택합니다.
4. *https://<FQDN>:8443/*을 예외로 추가합니다.
5. **Add Certificate(**인증서 추가**)**를 클릭한 다음 Firefox 브라우저를 새로 고칩니다.

Cisco ISE 릴리스 3.0부터는 지원되는 모든 Microsoft 릴리스에서 Agentless Posture(에이전트리스 포스처) 기능을 사용할 수 있습니다. 사용 중인 Cisco ISE 릴리스의 *Cisco ISE* 관리자 가이드에서 '컴플라이언스' 장의 '에이전트리스 상태' 항목을 참조하십시오.

스폰서, 게스트 및 내 디바이스 포털에 대해 검증된 운영체제 및 브라우저

이러한 Cisco ISE 포털은 다음과 같은 운영체제 및 브라우저 조합을 지원합니다. 이러한 포털을 사용하려면 웹 브라우저에서 쿠키를 활성화해야 합니다.

표 *7:* 검증된 운영체제 및 브라우저

지원되는 운영체제[5]	브라우저 버전
Google 안드로이드[6] 10.x, 9.x, 8.x, 7.x	• 네이티브 브라우저 • Mozilla Firefox • Google Chrome
Apple iOS 13.x, 12.x, 11.x	• Safari
Apple macOS 11, 10.15, 10.14, 10.13	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10	• Microsoft IE 11.x • Mozilla Firefox • Google Chrome

[5] 공식적으로 릴리스된 2개의 최신 브라우저 버전은 Microsoft Windows를 제외한 모든 운영체제에서 지원됩니다. 지원되는 Internet Explorer 버전은 표 14를 참조하십시오.

[6] 특정 디바이스에서 안드로이드 구현 시 개방형 액세스가 가능하기 때문에 Cisco ISE는 특정 안드로이드 OS 버전 및 디바이스 조합을 지원하지 않을 수 있습니다.

온보딩 및 인증서 프로비저닝을 위해 검증된 디바이스

BYOD 기능을 사용하려면 Cisco WLC(Wireless LAN Controller) 7.2 이상이 지원되어야 합니다. Cisco Identity Services Engine 릴리즈 노트에서 알려진 문제나 주의 사항을 확인하십시오.

참고 최신 Cisco 지원 클라이언트 운영체제 버전을 가져오려면 포스처 업데이트 정보를 확인합니다. 이렇게 하려면 다음을 수행합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Settings(설정)** > **Posture(포스처)** > **Updates(업데이트)**.
2. **Update Now(지금 업데이트)**를 클릭합니다.

표 *8: BYOD* 온보딩 및 인증서 프로비저닝 - 검증된 디바이스 및 운영체제

디바이스	운영 체제	단일 **SSID**	이중 **SSID(Open(열기) > PEAP(no cert) or Open(PEAP(인증서 없음) 또는 열기) > TLS(TLS))**	온보딩 방법
Apple iDevice	Apple iOS 13.x, 12.x, 11.x Apple iPad OS 13.x	예	예[7]	Apple 프로파일 구성(네이티브)
Google Android	10.x, 9.x, 8.x, 7.x	예[8]	예	Cisco Network Setup Assistant
Barnes & Noble Nook(안드로이드) HD/HD+[9]	—	—	—	—
Windows	Windows 10 EAP TEAP에는 Microsoft Windows 10 버전 2004(OS 빌드 19041.1) 이상이 필요합니다.	예[10]	예	2.2.1.53 이상
Windows	Mobile 8, Mobile RT, Surface 8 및 Surface RT	아니요	아니요	—
Apple macOS	Apple macOS 11, 10.15, 10.14, 10.13	예	예	2.2.1.43 이상

[7] 프로비저닝 후 보안 SSID로 연결

[8] 안드로이드 6.0 이상 버전을 사용하는 경우 Cisco SPW(Supplicant Provisioning Wizard)를 사용하여 시스템 생성 SSID를 수정할 수 없습니다. SPW에서 네트워크를 무시하라는 메시지가 표시되면 이 옵션을 선택하고 Back(뒤로) 버튼을 눌러 프로비저닝 플로우를 계속해야 합니다.

[9] Barnes & Noble Nook(안드로이드)는 Google Play Store 2.1.0이 설치되어 있는 경우 작동합니다.

[10] 연결을 위한 무선 속성을 구성할 때(**Security(**보안**) > Auth Method(**인증 방법**) > Settings(**설정**) > Validate Server Certificate(**서버 인증서 확인**))** 유효한 서버 인증서 옵션의 선택을 해제하십시오. 이 옵션을 선택하는 경우 올바른 루트 인증서를 선택해야 합니다.

검증된 보안 제품 통합(pxGrid 사용)

표 ***9:*** 검증된 보안 제품 통합***(pxGrid*** 사용***)***

제품	**Cisco ISE 3.1**	**Cisco ISE 3.0**	**Cisco ISE 2.7**	**Cisco ISE 2.6**
Cisco Firepower Management Center	Firepower Management Center 6.5를 이용한 Firepower Threat Defense Firepower Management Center 6.6을 이용한 Firepower Threat Defense Firepower Management Center 6.7을 이용한 Firepower Threat Defense Firepower Management Center 6.5를 이용한 Firepower Threat Defense Firepower Management Center 6.6을 이용한 Firepower Threat Defense Firepower Management Center 6.7을 이용한 Firepower Threat Defense	Firepower Management Center 6.5를 이용한 Firepower Threat Defense Firepower Management Center 6.6을 이용한 Firepower Threat Defense Firepower Management Center 6.5를 이용한 Firepower Threat Defense Firepower Management Center 6.6을 이용한 Firepower Threat Defense	Firepower Management Center 6.4를 이용한 Firepower Threat Defense	Firepower Management Center 6.4를 이용한 Firepower Threat Defense
Cisco Stealthwatch Management	Cisco Stealthwatch Management 7.1.2 Cisco Stealthwatch Management 7.3.2	Cisco Stealthwatch Management 7.1.2	Cisco Stealthwatch Management 7.0	Cisco Stealthwatch Management 6.9

제품	**Cisco ISE 3.1**	**Cisco ISE 3.0**	**Cisco ISE 2.7**	**Cisco ISE 2.6**
Cisco Web Security Appliance	Cisco Web Security Appliance 11.5.1	Cisco Web Security Appliance 11.5.1 Cisco Web Security Appliance 14.0 Cisco Web Security Appliance 14.5	Cisco Web Security Appliance 11.5.1 Cisco Web Security Appliance 11.8.3 Cisco Web Security Appliance 12.0.3 Cisco Web Security Appliance 12.5.3 Cisco Web Security Appliance 14.0.0 Cisco Web Security Appliance 14.5.0	—

참고 Cisco ISE 릴리스 3.1부터 모든 pxGrid 연결은 pxGrid 2.0을 기반으로 해야 합니다. pxGrid 1.0 기반(XMPP 기반) 통합은 릴리스 3.1부터 Cisco ISE에서 작동하지 않습니다.

WebSockets를 기반으로 하는 pxGrid 버전 2.0은 Cisco ISE 릴리즈 2.4에서 소개되었습니다. 잠재적인 통합 중단을 방지하려면 다른 시스템을 pxGrid 2.0 호환 버전으로 계획 및 업그레이드하는 것이 좋습니다.

검증된 **Cisco Digital Network Architecture Center** 릴리스

Cisco ISE와 Cisco DNA Center 통합 Cisco DNA Center에서 작동하도록 Cisco ISE를 구성하는 방법에 대한 자세한 내용은 *Cisco DNA Center* 설명서를 참조하십시오.

Cisco DNA Center와 Cisco ISE 호환성에 대한 자세한 내용은 *Cisco SD-Access* 호환성 매트릭스를 참조하십시오.

검증된 **Cisco Prime Infrastructure** 릴리스

Cisco Prime Infrastructure 릴리스 3.6 이상을 Cisco ISE 2.6 이상과 통합하여 Cisco ISE의 모니터링 및 보고 기능을 활용할 수 있습니다.

검증된 **Cisco Firepower Management Center** 릴리스

Cisco Firepower Management Center, 릴리스 6.4 이상은 Cisco ISE 2.6 이상과 통합할 수 있습니다.

검증된 **Cisco Stealthwatch Management** 릴리스

Cisco Stealthwatch Management, 릴리스 6.9 이상은 Cisco ISE 2.6 이상과 통합할 수 있습니다.

검증된 Cisco WAN 서비스 관리자 릴리스

Cisco WAN Service Administrator, 릴리스 11.5.1 이상은 Cisco ISE 2.7 이상과 통합할 수 있습니다.

위협 중심 NAC 지원

Cisco ISE는 다음과 같은 어댑터로 검증되었습니다.

- SourceFire FireAMP
- CTA(Cognitive Threat Analytics) 어댑터
- Rapid7 Nexpose
- Tenable Security Center
- Qualys(현재 TC-NAC 플로우에서는 Qualys Enterprise Edition만 지원)

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.

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2021 Cisco Systems, Inc. 모든 권리 보유.

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.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.