Cisco ID 서비스 엔진에 대한 릴리스 노트, 릴리스 3.0

참고

콘텐츠 허브(content.cisco.com)로 이동합니다. 여기서 Faceted Search(패싯 검색) 기능을 사용하여 원하는 콘텐츠를 정확하게 확대할 수 있으며, 즉시 참조할 수 있도록 맞춤형 PDF 문서를 즉시 생성하고 더 많은 것을 할 수 있습니다

무엇을 망설이십니까? 지금 content.cisco.com을 클릭하십시오!

그리고 이미 Content Hub(콘텐츠 허브)를 경험하고 있는 경우, 언제든지 알려 주십시오.

페이지에서 **Feedback(**피드백**)** 아이콘을 클릭하고 생각의 흐름에 맡기십시오.

소개

Cisco ISE(71Introduction)는 네트워크 리소스에 대한 보안 액세스를 제공하는 보안 정책 관리 플랫폼입니다. Cisco ISE를 사용하는 기업은 네트워크, 사용자 및 디바이스에서 실시간 상황별 정보를 수집할 수 있습니다. 관리자는 액세스 스위치, WLC(Wireless LAN Controller), VPN(Virtual Private Network) 게이트웨이 및 데이터 센터 스위치를 비롯한 다양한 네트워크 요소에 ID를 연결하는 방식으로 그러한 정보를 사용하여 능동적인 거버넌스 결정을 내릴 수 있습니다. Cisco ISE는 Cisco TrustSec 솔루션에서 정책 관리자 역할을 하며, TrustSec 소프트웨어 정의 세그먼테이션을 지원합니다.

Cisco ISE는 성능 특성이 다른 Secure Network Server 어플라이언스에서 사용 가능하며, VM(Virtual Machine)에서 실행할 수 있는 소프트웨어로도 제공됩니다. 더 나은 성능을 위해, 어플라이언스를 구축에 더 추가할 수 있습니다.

Cisco ISE는 독립형 및 분산형 구축을 지원하지만 중앙 집중식 컨피그레이션 및 관리를 지원하는 확장 가능한 아키텍처를 갖추고 있습니다. 또한 고유한 페르소나 및 서비스의 컨피그레이션 및 관리를 활성화하여, 네트워크에서 필요한 경우 서비스를 생성하고 적용할 수는 있지만 Cisco ISE 구축을 완벽하고 조정된 시스템으로 운영할 수 있습니다.

이 Cisco ISE 릴리스에서 지원되는 기능에 관한 자세한 내용은 Cisco ISE(Identity Services Engine) 관리자 설명서의 '라이선싱' 장을 참조하십시오.

cisco.com의 설명서에 액세스하려면, End-User Documentation(최종 사용자 설명서)로 이동하십시오.

Cisco ISE 릴리스 3.0의 새로운 기능은 무엇입니까?

Cisco ISE, 릴리스 3.0에서는 Essentials, Advantage 및 Premium 라이선스를 사용합니다.

라이선스 설치에 관한 자세한 내용은 Cisco ISE(Identity Services Engine) 관리자 설명서의 '라이선싱' 장을 참조하십시오.

새 기능은 기능에 필요한 라이선스에 따라 구성됩니다.

Essentials 라이선스

다음 기능을 사용하려면, Cisco ISE Essentials 라이선스가 필요합니다.

기능별 디버그 마법사

디버그 마법사에는 ISE 노드의 문제를 해결하는 데 사용할 수 있는 사전 정의된 디버그 템플릿이 포함되어 있습니다. 디버그 프로파일 및 디버그 로그를 구성할 수 있습니다.

비즈니스 성과: 이제 Cisco TAC는 Cisco ISE 구축의 여러 노드에서 디버그 로그를 쉽게 활성화할 수 있습니다. 이 기능을 사용하면, 문제를 더 빠르게 해결할 수 있습니다.

MFA(Multi-Factor Authentication)에 대한 SAML SSO

다단계 인증을 지원하도록, SAML 요청 제목의 인증 컨텍스트 값을 수정합니다.

비즈니스 성과: 이제 SAML 인증에서 다단계 인증을 지원합니다.

VMware Cloud on AWS(Amazon Web Services) 및 AVS(Azure VMware Solution)의 VMware 클라우드에서 Cisco ISE 지원

VMware 클라우드에 Cisco ISE를 설치하는 프로세스는 VMware 가상 컴퓨터에 Cisco ISE를 설치하는 프로세스와 정확히 동일합니다. 지원되는 가상 환경, 7 페이지의 내용을 참조하십시오.

비즈니스 성과: WS(Amazon Web Services) 및 AVS(Azure VMware Solution)의 VMware Cloud에서 호스팅할 수 있습니다.

ODBC ID 저장소에 대한 다중 속성 조회

ODBC ID 저장소를 추가하는 동안, **Advanced Settings(**고급 설정**)** 옵션을 클릭하여 다음 사전 아래의 속성을 **Fetch Attributes(**속성 가져오기**)** 저장 절차(사용자 이름 및 비밀번호 추가)의 입력 매개 변수로 사용합니다.

- RADIUS
- 디바이스
- 네트워크 액세스(AuthenticationMethod, 디바이스 IP 주소, EapAuthentication, EapTunnel, ISE Host Name(호스트 이름), 프로토콜, UserName, VN 및 WasMachineAuthenticated)

ODBC 데이터베이스에서 다음 출력 매개변수를 검색하도록 저장 절차를 구성할 수 있습니다.

- ACL
- Security Group(보안 그룹)
- VLAN(이름 또는 번호)

- 웹 리디렉션 ACL
- 웹 리디렉션 포털 이름

비즈니스 성과: 이러한 속성을 사용하여 권한 부여 프로파일을 구성할 수 있습니다. 예를 들어, 권한 부여 프로파일을 구성하여 수동으로 각 권한 부여 프로파일의 VLAN을 지정하는 대신에 지정된 입력 속성(예, MAC 주소, 사용자 이름, Calling-Station-ID 또는 디바이스 위치)을 기반으로 ODBC 데이터베이스에서 반환되는 VLAN을 사용할 수 있습니다.

Cisco ISE API 게이트웨이

Cisco ISE API 게이트웨이는 여러 Cisco ISE 서비스 API에 대한 Entry Point(엔트리 포인트) 역할을 하여 더 우수한 보안 및 트래픽 관리 기능을 제공하는 API 관리 솔루션입니다. 외부 클라이언트의 API 요청은 Cisco ISE의 API 게이트웨이로 라우팅됩니다. API 게이트웨이에 구성된 규칙에 따라, 요청은 서비스 API가 실행 중인 Cisco ISE 노드로 추가 전달됩니다.

비즈니스 성과**:** Cisco ACI 인프라와 결합된 Cisco SDA(Software Defined Access) 패브릭에 대한 정보 교환 및 도메인 간 자동화의 향상된 변환.

인증서 지문

인증서 핑거 프린팅 프로세스는 신뢰할 수 있는 인증서로 즉시 발급자 핑거 프린트 SHA256 인증서를 평가하는 데 사용됩니다. 이렇게 하면, 여러 인증서가 서로 다른 도메인을 지원하도록 보안 메커니즘이 적용됩니다. 인증서 핑거 프린팅을 통해, 802.1x 프로토콜에 대해 신뢰할 수 있는 인증서를 잠글 수도 있습니다.

비즈니스 성과**:** 여러 개의 신뢰할 수 있는 인증서에서 여러 도메인이 지원됩니다.

Passive Identity Service(패시브 ID 서비스)에 대한 MSRPC 프로토콜

Cisco ISE, 릴리스 3.0부터는 Passive Identity(패시브 ID)에 MS-Eventing API 또는 MSRPC(Microsoft Remote Procedure Call) 프로토콜을 사용할 수 있습니다. MSRPC 프로토콜을 사용하여, 노드 통신을 설정하고 Cisco ISE에서 노드 사이의 하트비트를 모니터링합니다. 이 옵션은 Passive Identity(패시브 ID) 서비스용 WMI 프로토콜과 함께 사용할 수 있습니다.

MSRPC 프로토콜은 Cisco ISE 또는 Cisco ISE-PIC가 여러 도메인 컨트롤러에서 이벤트를 수집하고 모니터링할 때 신뢰할 수 있는 메커니즘을 제공합니다. 또한 Active Directory Domain Controllers(도메인 컨트롤러) 사용자 로그인 이벤트의 레이턴시를 줄입니다.

비즈니스 성과**:** DC 이벤트를 모니터링하기 위한 안정적인 메커니즘을 제공합니다.

상태 확인

구축의 모든 노드를 진단하기 위해 온디맨드 상태 확인 옵션이 도입되었습니다. 작업 전에 모든 노드에서 상태 확인을 실행하면, 다운 타임 또는 차단을 유발할 수 있는 중요한 문제를 식별할 수 있습니다. 상태 확인은 모든 종속 구성 요소의 작업 상태를 제공합니다. 구성 요소에 장애가 발생하면, 문제를 해결하기 위한 문제 해결 권장 사항이 즉시 제공되므로 작업이 원활하게 실행됩니다.

업그레이드 프로세스를 시작하기 전에, 상태 확인을 실행해야 합니다.

비즈니스 성과**:** 다운 타임 또는 차단을 방지하기 위해 중요한 문제를 파악합니다.

Telemetry(텔레메트리) 업데이트

추가 네트워크 통계가 수집됩니다.

비즈니스 성과: 고객 네트워크에 대해 더 많은 정보를 수집할수록, 제품을 개선하는 방법에 대한 분석을 더 잘 수행할 수 있습니다.

TCP Dump(TCP 덤프) 개선 사항

이제 TCP Dump(TCP 덤프) 파일을 더 많이 제어할 수 있습니다. 추가 인터페이스에서 TCP Dump(TCP 덤프)를 실행할 수도 있습니다.

비즈니스 성과: 이제 TCP 트래픽에 대한 데이터 수집이 더 쉬워졌습니다.

Azure Active Directory로 사용자를 인증하기 위한 ROPC(Resource Owner Password Credentials) 흐름

ROPC(Resource Owner Password Credentials) 플로우를 통해 Cisco ISE는 클라우드 기반 ID 제공자가 있는 네트워크에서 권한 부여 및 인증을 수행할 수 있습니다. 이는 제어된 도입 기능입니다. 프로덕션 환경에서 사용하기 전에, 테스트 환경에서 이 기능을 철저하게 테스트하는 것이 좋습니다.

비즈니스 성과: ROPC 흐름을 통해 Cisco ISE는 Azure Active Directory 사용자를 인증하고 인증할 수 있습니다.

Interactive Help(대화형 도움말)

Interactive Help(대화형 도움말)은 작업을 쉽게 완료할 수 있는 팁과 단계별 지침을 제공합니다.

비즈니스 성과: 최종 사용자가 워크플로를 쉽게 이해하고 작업을 쉽게 완료할 수 있습니다.

어드밴티지 라이선스

다음 기능을 사용하려면, Cisco ISE Advantage 라이선스가 필요합니다.

새 pxGrid 페이지

새 pxGrid 인터페이스에는 pxGrid v1과 pxGrid v2를 구분하는 새 페이지가 있습니다. 세션 및 클라이언트 정보가 포함된 새로운 Summary(요약) 창이 있습니다.

비즈니스 성과: pxGrid 세션을 관리할 때 워크플로를 개선합니다.

참고 레거시 XMPP(Extensible Messaging and Presence Protocol)를 사용하는 pxGrid 1.0은 유지 보수 모드이며, 곧 사용이 중단됩니다. Cisco ISE 릴리스 2.4에서 pxGrid 2.0을 도입했습니다. pxGrid 2.0은 단순하고 표준화 된 애플리케이션-애플리케이션 간 통신 인터페이스인 REST 및 Websocket 프로토콜을 사용합니다. 파트너는 pxGrid 클라이언트 구현을 이러한 새 프로토콜로 전환하는 것이 좋습니다.

pxGrid 2.0으로의 전환을 권장하는 이유에 대한 자세한 내용은 pxGrid (Cisco Platform Exchange Grid 학습 시작)를 참조하십시오.

Desktop Device Manager(데스크톱 디바이스 관리자)에서 베이스라인 정책 컨피그레이션

Cisco ISE 릴리스 3.0으로 업그레이드 할 때는 루트 패치를 사용하여 연결된 Desktop Device Manager(데스크톱 디바이스 관리자) 서버에서 컨피그레이션 베이스라인 정책을 선택하지 않는 것이 좋습니다.

또한 동글, 도킹 스테이션 또는 MAC 주소 임의 지정 기술을 사용하는 경우, MAC 주소 대신 디바이스 식별자로 Windows 엔드포인트를 확인하여 정확성을 높일 수 있습니다.

비즈니스 성과**:** Desktop Device Manager 서버에서 생성된 컨피그레이션 베이스라인 정책을 사용하여 엔드포인트 규정 준수를 확인할 수 있습니다. 엔드포인트 식별의 정확도를 높이려면, MAC 주소 대신 디바이스 식별자를 사용하십시오.

Cisco ISE ACI-SDA와 VN 인식 통합

Cisco ISE 릴리스 3.0은 Cisco ACI 인프라와 결합된 Cisco SDA(Software Defined Access) 패브릭에 대한 정보 교환 및 도메인 간 자동화의 향상된 변환을 제공합니다. 이 구현에서는 EPG 및 SGT 정보의 교환 및 변환, SDA VN(Virtual Network)을 Cisco ACI 패브릭으로 확장, SDA 및 ACI 패브릭 데이터 플레인 자동화, IP-SGT 바인딩 교환, pxGrid 및 SXP 도메인로 바인딩 전송을 지원합니다.

비즈니스 성과**:** 향상된 보안 및 트래픽 관리.

안티바이러스 및 안티멀웨어의 최소 버전

Cisco ISE 릴리스 3.0부터는 네트워크의 엔드포인트에 대한 안티바이러스 및 안티멀웨어의 최소 버전을 설정하는 포스처 정책을 생성할 수 있습니다. 이 정책은 엔드 포인트가 네트워크 정책의 안티바이러스 및 안티멀웨어의 최소 버전을 준수하도록 합니다. 또한 새로운 버전의 안티바이러스 및 안티멀웨어로 조건을 자동으로 업데이트하므로, 조건을 수정하는 데 필요한 수동 작업이 줄어 듭니다.

비즈니스 성과**:** 엔드포인트가 네트워크 정책을 준수하므로, 보안이 강화되었습니다.

포스처 세션 공유

포스처 상태는 PSN 간에 공유됩니다. 상태는 구성할 수 없습니다. 항상 켜져 있습니다.

비즈니스 성과**:** 다른 PSN으로 전환할 때 클라이언트 연결이 포스처를 다시 실행할 필요가 없습니다.

Agentless Posture(에이전트리스 포스처)

이 새로운 포스처 유형은 SSH를 통해 클라이언트에 에이전트를 전달하며 포스처가 완료되면 선택적으로 클라이언트를 제거합니다. AnyConnect는 필요하지 않습니다.

비즈니스 성과**:** 공간 부족 및 임시 포스처 에이전트가 고객에게 표시되지 않습니다.

다중 DNAC 지원

Cisco DNA 센터 시스템은 엔드포인트를 25,000~10,000개까지 확장할 수 없습니다. Cisco ISE는 2백만 개의 엔드포인트로 확장할 수 있습니다. 현재는 하나의 Cisco DNA Center 시스템과 하나의 Cisco ISE 시스템만 통합할 수 있습니다. 대규모 DNA ISE 구축에서는 여러 DNA Center 클러스터를 단일 Cisco ISE와 통합하여 이점을 얻을 수 있습니다. Cisco는 이제 Cisco ISE 구축당 다중 Cisco DNA Center 클러스터(Multi-DNAC라고도 함)를 지원합니다.

비즈니스 성과**:** Cisco DNA Center의 액세스 제어 앱을 위한 이 기능을 사용하면, 최대 4개의 Cisco DNA Center 클러스터를 단일 Cisco ISE 시스템과 통합할 수 있습니다.

Premier 라이선스

다음 기능을 사용하려면, Cisco ISE Premier 라이선스가 필요합니다.

Endpoint Scripts(엔드포인트 스크립트) 마법사

Endpoint Scripts(엔드포인트 스크립트) 마법사를 사용하면, 연결된 엔드포인트에서 스크립트를 실행하여 조직의 요구 사항을 준수하는 관리 작업을 수행할 수 있습니다. 여기에는 사용하지 않는 소프트웨어 제거, 프로세스 또는 애플리케이션 시작 또는 종료, 특정 서비스 활성화 또는 비활성화와 같은 작업이 포함됩니다.

비즈니스 성과: 조직의 요구 사항을 준수하기 위해 연결된 엔드포인트에서 관리 작업을 쉽게 수행합니다.

시스템 요구 사항

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

이 Cisco ISE 3300 릴리스의 하드웨어 플랫폼 및 설치에 대한 자세한 내용은 *Cisco ISE(Identity Services Engine), 릴리스 1.2 하드웨어 설치 설명서*를 참조하십시오.

지원되는 하드웨어

Cisco ISE, 릴리스 3.0은 다음 플랫폼에서 설치 및 실행할 수 있습니다.

표 ***1:*** 지원되는 플랫폼

하드웨어 플랫폼	컨피그레이션
Cisco SNS-3515-K9(소형)	어플라이언스 하드웨어 사양은 *Cisco SNS(Secure Network Server) 어플라이언스 하드웨어 설치 설명서*를 참조하십시오.
Cisco SNS-3595-K(대형)	
Cisco SNS-3615-K9(소형)	
Cisco SNS-3655-K9(중간)	
Cisco SNS-3695-K9(대형)	

하드웨어 플랫폼	컨피그레이션
Cisco ISE-VM-K9(VMware, Linux KVM, Microsoft Hyper-V) VMware ESXi 5.x, 6.x, 7.x	• CPU 및 메모리 권장 사항은 *Cisco ISE(Identity Services Engine) 설치 설명서*의 "VMware Appliance Sizing Recommendations(VMware 어플라이언스 크기 조정 권장 사항)" 섹션을 참조하십시오. • 권장 하드 디스크 크기는 *Cisco ISE(Identity Services Engine) 설치 설명서*의 "Disk Space Requirements(디스크 공간 요구 사항)" 섹션을 참조하십시오. • NIC-1GB NIC 인터페이스가 필요합니다. 최대 6개의 NIC를 설치할 수 있습니다.

설치 후에는 위 표에 나열된 플랫폼에서 Administration(관리), Monitoring(모니터링) 및 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, 릴리스 2.4 이상에서 Cisco SNS(Secured Network Server) 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 5.x, 6.x, 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 구축되니 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.

- Microsoft Windows Server 2012 R2 이상의 Microsoft Hyper-V
- QEMU 1.5.3-160의 KVM

FIPS(Federal Information Processing Standard) 모드 지원

Cisco ISE는 임베디드 FIPS(Federal Information Processing Standard) 140-2- 검증된 암호화 모듈, Cisco FIPS Object Module 버전 6.2(인증서 # 2984)를 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

지원되는 브라우저

지원되는 Admin Portal(관리자 포털)용 브라우저는 다음과 같습니다.

- Mozilla Firefox 80 이하 버전

- Mozilla Firefox ESR 60.9 이하 버전
- Google Chrome 85 이하 버전
- Microsoft Internet Explorer 11.x

확인된 External Identity Sources(외부 ID 소스)

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

External Identity Source(외부 ID 소스)	OS/버전
Active Directory [1] [2]	
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2 [3]	—
Microsoft Windows Active Directory 2016	—
Microsoft Windows Active Directory 2019 [4]	—
LDAP 서버	
SunONE LDAP Directory Server	버전 5.2
OpenLDAP Directory Server	버전 2.4.23
모든 LDAP v3 호환 서버	—
토큰 서버	
RSA ACE/Server	6.x Series
RSA 인증 관리자	7.x 및 8.x Series
RADIUS RFC 2865와 호환되는 모든 토큰 서버	—
SAML(Security Assertion Markup Language) SSO(Single Sign-On)	
Microsoft Azure	—
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	—

External Identity Source(외부 **ID** 소스)	**OS**/버전
보안 인증	8.1.1
모든 SAMLv2 호환 ID 제공자	—
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	—

[1] Cisco ISE OCSP 기능은 Microsoft Windows Active Directory 2008 이상에서만 사용할 수 있습니다.

[2] ISE에는 최대 200개의 도메인 컨트롤러만 추가할 수 있습니다. 제한을 초과하면, 다음 오류가 표시됩니다.

```
생성 오류<DC FQDN> -DC 수 허용되는 최대 200개 초과
```

[3] Cisco ISE는 Microsoft Windows Active Directory 2012 R2의 모든 레거시 기능을 지원하지만, Protective User Groups와 같은 2012 R2의 신기능은 지원하지 않습니다.

[4] Cisco ISE는 Cisco ISE 릴리스 2.6.0.156 패치 4 이상에서 제공되는 Microsoft Windows Active Directory의 모든 레거시 기능을 지원합니다.

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

지원되는 안티바이러스 및 안티멀웨어 제품

ISE Posture Agent에서 지원하는 안티바이러스 및 안티멀웨어 제품에 대한 자세한 내용은 *Cisco ISE(Identity Services Engine)* 호환성 설명서의 Cisco AnyConnect ISE Posture 지원 차트를 참조하십시오.

검증된 **OpenSSL** 버전

Cisco ISE는 OpenSSL 1.0.2.x(CiscoSSL 6.0)로 검증되었습니다.

알려진 제한 사항 및 해결 방법

업그레이드 후 **LDAP** 서버 재구성

제한 사항

기본 호스트네임 또는 IP가 업데이트되지 않아 인증이 실패합니다. Cisco ISE 구축과 관련하여 구축 ID가 재설정되는 경향이 있기 때문입니다.

조건

Connection(연결**)** 창에서 **Specify server for each ISE node(**각 **ISE** 노드에 대해 서버 지정**)** 옵션을 활성화하는 경우. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP** > **Add(**추가**)** 또는 기존 서버를 선택한 다음, PSN이 있는 Cisco ISE 구축을 업그레이드하면 구축 ID가 재설정되는 경향이 있습니다.

해결 방법

각 노드에 대해 LDAP 서버 설정을 재구성합니다. 자세한 내용은 "Cisco Identity Services Engine 관리자 설명서, 릴리스 2.4"의 외부 ID 저장소를 사용한 **Cisco ISE**에 대한 관리 액세스 장의 *LDAP ID* 소스 설정 섹션을 참조하십시오.

일본어 온라인 도움말

Cisco ISE에서 일본어를 사용하도록 현지화 설정을 구성한 경우, 온라인 도움말에는이 릴리스에 도입된 새로운 기능에 대한 정보가 포함되어 있지 않습니다. 이러한 기능에 대한 자세한 내용은 *Cisco ISE* 관리 설명서, 릴리스 *3.0*을 참조하십시오.

업그레이드 정보

- 라이선스 변경 사항, 12 페이지
- 업그레이드 절차 전제 조건

참고 핫 패치를 설치한 경우에는 핫 패치를 롤백한 후에 업그레이드 패치를 적용합니다.

릴리스 **3.0**으로 업그레이드

다음 릴리스는 곧바로 Cisco ISE, 릴리스 3.0으로 업그레이드할 수 있습니다.

- 2.4
- 2.6
- 2.7

Cisco ISE, 릴리스 1.2 패치 14보다 낮은 버전인 경우, 먼저 위에 표시된 릴리스 중 하나로 업그레이드한 다음 릴리스 1.4로 업그레이드해야 합니다.

참고 업그레이드를 시작하기 전에, 기존 버전의 최신 패치로 업그레이드하는 것이 좋습니다.

업그레이드 패키지

업그레이드 패키지 및 지원되는 플랫폼에 대한 정보는 Cisco ISE Software Download(Cisco ISE 소프트웨어 다운로드)에서 확인할 수 있습니다.

라이선스 변경 사항

Base, Plus, Apex 등 Cisco ISE, 릴리스 2.x에 사용되는 라이선스가 새 라이선스 유형으로 교체되었습니다. Cisco ISE, 릴리스 3.0에서는 Essentials, Advantage 및 Premium 라이선스를 사용합니다. *Cisco ISE(Identity Services Engine) 관리자 설명서*의 "라이선싱" 장을 참조하십시오.

Cisco ISE, 릴리스 3.0에서 라이선스 사용을 활성화하려면, CSSM(Cisco Smart Software Manager)을 통해 기존 스마트 또는 기존 라이선스를 새 라이선스 유형으로 변환해야 합니다.

업그레이드 절차 전제 조건

- 구성된 데이터를 필수 ISE 버전으로 업그레이드할 수 있는지 확인하려면, ISE 소프트웨어를 업그레이드하기 전에 URT(Upgrade Readiness Tool)를 실행합니다. 대부분의 업그레이드 실패는 데이터 업그레이드 문제로 발생합니다. URT는 실제 업그레이드하기 전에 데이터를 검증하도록 설계되었으며, 가능한 경우 문제를 보고하고 해결하려고 시도합니다. URT는 *Cisco ISE Download Software Center(소프트웨어 센터 다운로드)*에서 다운로드 할 수 있습니다.
- 업그레이드를 시작하기 전에, 모든 관련 패치를 설치하는 것이 좋습니다.

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

Telemetry

설치 후 관리 포털에 처음 로그인하면, Cisco ISE Telemetry 배너가 화면에 나타납니다. 이 기능을 사용하여, Cisco ISE는 구축, 네트워크 액세스 디바이스, 프로파일러 및 사용 중인 기타 서비스에 대한 민감하지 않은 정보를 안전하게 수집합니다. 수집되는 데이터는 향후 릴리스에서 보다 나은 서비스와 추가적인 기능을 제공하는 데 사용됩니다. 텔레메트리 기능은 기본값으로 활성화됩니다. 어카운트 정보를 비활성화하거나 수정하려면, Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **> Settings(**설정**) > Network Settings Diagnostics(**네트워크 설정 진단**) > Telemetry(**텔레메트리**)**를 선택합니다. 어카운트는 각 구축에서 고유합니다. 각 관리자 사용자가 별도로 제공할 필요는 없습니다.

Telemetry(텔레메트리)는 Cisco ISE의 상태 및 기능에 대한 유용한 정보를 제공합니다. Cisco에서는 텔레메트리를 사용하여 Cisco ISE를 구축한 IT 팀의 어플라이언스 라이프 사이클 관리를 개선합니다. 제품 팀은 이 데이터를 수집하여 이 고객에게 더 나은 서비스를 제공할 수 있습니다. 이 데이터 및 관련 통찰력을 통해 Cisco는 잠재적인 문제를 사전에 파악하고, 서비스 및 지원을 개선하며, 새로운 기

능과 기존 기능에서 추가 가치를 수집하기 위한 논의를 진행하고, 라이선스 엔타이틀먼트 및 향후 갱신에 대한 인벤토리 보고서를 통해 IT 팀을 지원합니다.

기능이 비활성화된 후 Cisco ISE가 텔레메트리 데이터 공유를 중지하려면, 최대 24 시간이 걸릴 수 있습니다.

수집되는 데이터 유형에는 Product Usage Telemetry(제품 사용 Telemetry) 및 Cisco Support Diagnostics(Cisco 지원 진단)가 있습니다.

컨피그레이션 사전 요구 사항

- 관련 Cisco ISE 라이선스 요금을 지불해야 합니다.
- 최신 패치를 설치해야 합니다.
- Cisco ISE 소프트웨어 기능이 활성 상태여야 합니다.

ISE 구성을 시작하려면, 다음 리소스를 참조하십시오.

- Cisco ISE 시작하기
- YouTube의 Cisco ISE 채널 비디오
- *Cisco ISE* 및 *WSA* 통합 설명서
- *Cisco ISE(Identity Services Engine)* 관리자 설명서

모니터링 및 문제 해결

시스템 모니터링 및 문제 해결에 대한 자세한 내용은 *Cisco ISE(Identity Services Engine)* 관리자 설명서의 "Cisco ISE 모니터링 및 문제 해결" 섹션을 참조하십시오.

주문 정보

자세한 Cisco ISE 주문 및 라이선싱 정보는 Cisco ISE(Identity Services Engine) 주문 설명서를 참조하십시오.

Cisco ISE와 Cisco Digital Network Architecture Center의 통합

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.

Cisco AI 엔드포인트 분석

Cisco DNA 엔드포인트 분석은 엔드포인트 프로파일링 정확도를 개선하는 Cisco DNA 센터의 솔루션입니다. 세분화된 엔드포인트 식별을 제공하고, 레이블을 다양한 엔드포인트에 할당합니다. 심층 패킷 검사를 통해 수집된 정보와 Cisco ISE, Cisco SD-AVC 및 네트워크 디바이스와 같은 소스의 프로브를 분석하여 엔드포인트 프로파일링을 수행합니다.

Cisco 인공 지능 엔드포인트 분석은 인공 지능 및 머신 러닝 기능을 사용하여 유사한 특성의 엔드포인트를 직관적으로 그룹화합니다. IT 관리자는 이러한 그룹을 검토하고 레이블을 할당할 수 있습니다. Cisco ISE 어카운트를 온프레미스 Cisco DNA 센터에 연결하는 경우, Cisco ISE에서 이러한 엔드포인트 레이블을 사용할 수 있습니다.

Cisco ISE 관리자는 Cisco AI Endpoint Analytics의 이 엔드포인트 레이블을 사용하여 맞춤형 권한 부여 정책을 생성할 수 있습니다. 이러한 권한 부여 정책을 통해 엔드포인트 또는 엔드포인트 그룹에 대한 적절한 액세스 권한 집합을 제공할 수 있습니다.

새 패치 다운로드 및 설치

Cisco ISE에 패치를 적용하는 데 필요한 패치 파일을 가져오려면, https://software.cisco.com/download/home에서 Cisco Download Software(소프트웨어 다운로드) 사이트(Cisco.com 로그인 자격 증명을 제공해야 함)에 로그인하고, **Security(보안) > Access Control and Policy(액세스 제어 및 정책) > Cisco ISE(Identity Services Engine) > Cisco Identity Services Engine Software**로 이동하며, 패치 파일의 복사본을 로컬 시스템에 저장합니다.

시스템에 패치를 적용하는 방법에 대한 지침은 *Cisco Identity Services Engine* 관리자 설명서의 "소프트웨어 패치 설치" 섹션을 참조하십시오.

CLI를 사용하여 패치를 설치하는 방법에 대한 지침은 *Cisco ISE(Identity Services Engine) CLI* 참조 설명서의 "패치 설치" 섹션을 참조하십시오.

참고 릴리스 2.4 패치 4 이상을 설치하는 경우, 커널 업그레이드 중에 CLI 서비스를 일시적으로 사용할 수 없게 됩니다. 이 시간에 CLI에 액세스하는 경우, CLI에는 Stub Library를 열 수 없음 오류 메시지가 표시됩니다. 그러나 패치 설치가 완료되면, CLI 서비스를 다시 사용할 수 있습니다.

경고

Caveats(경고) 섹션에는 버그 ID와 버그에 대한 간단한 설명이 포함되어 있습니다. 특정 경고에 대한 증상, 조건 및 해결 방법에 대한 자세한 내용은 Cisco BST(Bug Search Tool)를 사용하십시오. 버그 ID는 영숫자로 정렬됩니다.

참고 미결 경고(Open Caveats) 섹션에는 현재 릴리스에 적용되고, Cisco ISE 3.0 이전 릴리스에 적용될 수 있는 공개 경고가 나열되어 있습니다. 이전 릴리스에서 열려 있지만, 여전히 확인할 수 없는 경고는 해결될 때까지 모든 향후 릴리스에 적용됩니다.

Bug Toolkit의 온라인 후속 제품인 BST는 네트워크 위험 관리 및 디바이스 문제 해결의 효율성을 개선하도록 설계되었습니다. 제품, 릴리스 또는 키워드를 기준으로 버그를 검색하고, 버그 상세정보, 제품 및 버전과 같은 주요 데이터를 집계할 수 있습니다. 이 툴에 대한 자세한 내용은 http://www.cisco.com/web/applicat/cbsshelp/help.html에 있는 Help(도움말) 페이지를 참조하십시오.

Cisco ISE 릴리스 3.0의 해결된 경고(Resolved Caveats)

고지 ID 번호	설명
CSCuo02920	ISE가 access-reject에서 구성된 Radius AVP 18을 반환하지 않음
CSCuz02795	홈 페이지를 새로 고칠 때 GET-BY-ID 구현되지 않음 예외
CSCva44035	실시간 인증의 VPN 사용자의 경우에는 ISE에 MAC 주소 대신에 IP 주소가 표시됩니다.
CSCvb55884	ISE RBAC 네트워크 디바이스 유형/위치 보기가 작동하지 않음
CSCvd38796	AD가 authC 및 authZ에 모두 사용되는 경우, RA-VPN/CWA에 대해 검색된 AD 도메인 특성이 없음
CSCve89689	MNT API는 특수 문자를 지원하지 않음
CSCvf30470	3.6.11362.2 규정 준수 모듈로 업그레이드한 후 MAC OX 실패
CSCvg50777	nas-update=true 어카운팅 속성으로 인해, 세션이 삭제되지 않습니다.
CSCvh77224	ENH // HTTPS Proxy(HTTPS 프록시)를 사용한 Smart License 등록 실패
CSCvi35647	다중 노드 구축에서 PSN 간에 포스처 세션 상태를 공유해야 함
CSCvi62805	CSCvi62805 ISE ODBC가 구성된 저장 절차에 따라 MAC 주소를 변환하지 않음
CSCvj47301	노드 그룹 멤버에 연결할 수 없는 경우, ISE가 CoA를 활성 준수 세션에 전송합니다.
CSCvj59836	IOS 디바이스용 온보드 포털의 오타
CSCvj77817	2.3P4, 2.4P3 업그레이드가 OS 업그레이드 중에 실패함
CSCvk04307	ISE 게스트/BYOD 포털 재시도가 1.1.1.1로 리디렉션됨
CSCvk50684	호스트네임 변경 시 RADIUS DTLS 및 포털 사용이 새 자체 서명 인증서에 할당되지 않음
CSCvn02461	Cisco IP Phone용 프로파일러 업데이트 포함-8832,7832
CSCvn12644	AD 속성에 대한 정책 평가 중에 ISE가 충돌함
CSCvn48096	모든 Context Visibility(상황 가시성) 페이지에서 Checkbox All(모두 적용) 엔드포인트 확인란이 선택되지 않음

고지 ID 번호	설명
CSCvn73740	엔드포인트 프로파일이 알 수 없음으로 설정된 EAP-TLS 인증이 두 번째 권한 부여에서 실패합니다.
CSCvn99149	요청 캐시 제어를 비공개, No-cache 및 No-store로 설정
CSCvo15770	주소가 Context Visibility(상황 가시성)에 HTML 코드로 표시됨
CSCvo22887	ISE 2.4 URT에서 노드가 지원되는 어플라이언스에 있는지 확인하지 않음
CSCvo28970	Cisco 임시 에이전트 사용 시 AnyConnect에 Cisco NAC Agent 오류 표시
CSCvo84056	Self-Reg Success page(셀프 등록 성공 페이지)의 "사용자 이름/비밀번호" 활성화 또는 비활성화가 페이지 맞춤화에 포함되지 않음
CSCvo87602	openldap rpm이 2.4.44 버전을 실행 중인 ISE 노드의 메모리 누수
CSCvp42493	게스트 ERS API "SearchResult" 총계가 다른 API와 일치하지 않습니다.
CSCvp59038	src ip 주소가 169.254.2.2인 다른 ISE 노드로 RST를 전송하는 ISE 보조 PAN 노드
CSCvp61452	[ENH] 패치 설치 단계 중에 아카이브 제거
CSCvp85813	ISE TACACS livelogs에는 특정 NAS IP 주소를 사용하여 필터링할 수 있는 옵션이 없습니다.
CSCvp88443	새 Logical Profile(논리적 프로파일)이 Authz Policy Exceptions(Authz 정책 예외)에서 사용되는 경우에도, ISE CoA가 전송되지 않습니다.
CSCvp93322	수명(Longevity) 테스트 중 MNT에서 상당한 메모리 증가
CSCvq12204	ISE 2.4 SNMPv3 사용자가 다시 로드된 후 잘못된 해시가 추가되어 SNMPv3 인증이 실패했습니다.
CSCvq13431	포스처 및 RADIUS 플로우 중에 컨텍스트 특성을 가져오는 동안, ISE PSN 노드 충돌
CSCvq43600	비활성화된 PSN 페르소나이지만, TACACS 포트 49가 계속 열려 있습니다.
CSCvq48396	복제 실패 알람이 생성되었으며, ise-psc.log에 ORA-00001 예외가 표시됨
CSCvq61089	SAML 인증을 통해 BYOD 온보딩 후 My Device Portal(내 디바이스 포털)에 디바이스가 표시되지 않음
CSCvq70247	셀프 등록 게스트 포털의 미리보기에 "등록 코드" 레이블이 표시되지 않음
CSCvq88821	AP에 연결된 액세스 스위치의 SNMP 트랩으로 인해, 잘못된 프로파일링이 발생합니다.

고지 ID 번호	설명
CSCvq90601	EAP 연결: Dynamic Attribute(동적 속성) 값을 사용할 수 없습니다.
CSCvr07294	RADIUS 인증 및 RADIUS 계정 보고서 성능이 느림
CSCvr22373	ENH: 기본 이벤트 로그 API 지원, Passive ID(패시브 ID) 기능을 위한 EVT API
CSCvr39943	CTA 클라우드에서 TC-NAC 어댑터로 수신되는 위협 이벤트에 대한 빈 작업 과정
CSCvr40545	개인 키 암호화에 실패한 경우, 공유 암호 없이 EAP-FAST 인증에 실패했습니다.
CSCvr40574	ISE GUI에서 개인 키 암호화에 오류가 발생하지 않은 경우, ISE GUI에서 내보내기에 실패했습니다.
CSCvr44495	pxGrid가 MnT 이벤트를 게시하지 않음
CSCvr48726	[enh] SCCM에 대한 컴플라이언스 디바이스 재인증 쿼리의 시간 간격 증가
CSCvr68432	2.4P10 엔드포인트가 REST를 통해 추가되면, "수정" 모드에서만 정책 할당이 표시됨
CSCvr68971	ISE IP 라우팅 우선 순위 문제
CSCvr70044	높은 로드 중에 ISE Posture Module에서 "정책 서버가 탐지되지 않음"
CSCvr81384	네트워크 디바이스 CSV 가져오기 실패, 이유 없이 프로세스 자동 중단
CSCvr83696	ISE: Account OU(어카운트 OU)를 변경한 후, 캐시된 AD OU가 새 OU보다 우선함
CSCvr84143	ISE 게스트 OS에서 tzdata를 업데이트해야 함
CSCvr85363	사용자 API로 인한 ISE 앱 충돌
CSCvr87373	ACI 매핑이 SXP pxGrid 항목에 게시되지 않음
CSCvr95948	ISE가 연결 중단 후, 외부 syslog 연결을 재설정하지 못함
CSCvr96003	SYSAUX 테이블 공간이 AWR 및 OPSSTAT 데이터로 채워지고 있음
CSCvs03810	사용자가 두 번 다르게 입력된 경우, ISE가 RADIUS 보고서에 올바른 사용자를 표시하지 않음
CSCvs04433	ISE: TACACS: TACACS+에서 PSN 충돌
CSCvs05260	매일 오전 1시에 앱 서버 및 EST 서비스 충돌/재시작

고지 ID 번호	설명
CSCvs07344	ISE: 2.4 패치 9의 컨피그레이션 재설정이 정상적으로 완료되었더라도 오류가 발생합니다.
CSCvs09981	ISE의 그룹 노드 사이의 MAR 캐시 확인으로 인해, 실패한 COA를 필터링하는 기능 추가
CSCvs19481	Cisco ISE(Identity Services Engine) 사이트 간 스크립팅 취약점
CSCvs23628	규칙이 일치한 후에도 정책 엔진은 모든 Policy Sets(정책 집합)를 계속 평가
CSCvs25258	무차별 비밀번호 공격에 대한 동작 개선
CSCvs25569	잘못된 Root CA(루트 CA) 인증서가 수락됨
CSCvs36036	사용자가 IPv4(또는 IPv6)를 선택하는 경우에도, ISE 2.6에서는 dACL 구문에서 여러 개의 빈 줄을 허용해야 합니다.
CSCvs36150	ISE 2.x Network Device(네트워크 디바이스) 로딩이 중단됨
CSCvs36758	ISE 2.6에서 2개의 괄호로 CRL URL을 구성할 수 없음
CSCvs38883	오래된 데이터를 푸시하는 TrustSec 매트릭스
CSCvs39633	NAD 그룹 CSV 가져오기에서는 설명 필드에 지원되는 모든 문자를 허용해야 합니다.
CSCvs39880	Xms 값의 관리 노드에 대한 높은 로드
CSCvs40406	신뢰할 수 있는 CA 인증서를 제거하는 동안, SEC_ERROR_BAD_DATABASE가 시스템/앱 디버그 로그에 표시됨
CSCvs41571	Self-Registered Guest Portal(셀프 등록된 게스트 포털)에서 게스트 유형 설정을 저장할 수 없음
CSCvs42072	Static Group Assignment(정적 그룹 할당)
CSCvs42441	SMS 및 LDAP 페이지의 서버에서 반환된 서비스 계정 비밀번호
CSCvs42758	특정 조건에서 CRL이 만료됨
CSCvs44006	Cisco ISE(Identity Services Engine) 사이트 간 스크립팅 취약점
CSCvs44795	ISE가 SGT를 올바르게 업데이트하지 않음
CSCvs46274	RADIUS 계정 관리 보고서가 작동하지 않음-어카운팅 관리 레코드가 표시되지 않음
CSCvs46399	url-redirect에 대한 AuthZ 프로파일 고급 프로파일에서 맞춤형 HTTPS 대상을 허용하지 않음

고지 ID 번호	설명
CSCvs46853	DNA-C와 통합하는 동안, CN이 동일한 ISE 2.6 CA 인증서가 신뢰할 수 있는 저장소에서 제거됨
CSCvs46998	조건이 라이브러리에서 사라졌지만 여전히 DB에 있음
CSCvs47941	ISE2.6에서 내부 CA 및 키를 가져오지 못함
CSCvs50437	ISE 버전은 새 Oracle 데이터베이스와 호환되지 않는 이전 JDBC 버전(11.2.0.3)을 사용함
CSCvs51296	ISE에서는 Command Sets(명령 집합) 아래에 명령 앞에 공백을 삽입할 수 있음
CSCvs51519	NFS 마운트로 인해 충돌 발생
CSCvs51537	암호화 키에 대한 특수 문자로 백업이 트리거되지 않음
CSCvs52031	MACAdress API가 작동하지 않음(API/mnt/Session/MACAddress)
CSCvs53606	ISE 2.4: 관리자 로그인 보고서, 인증서 기반 관리자 인증 사용 시 인증 실패
CSCvs55464	스폰서 포털에서 새 사용자를 생성하면, "invalid input"이 표시됨
CSCvs55594	Days to Expiry(만료까지 남은 일 수) 값(0)이 임의 인증으로 표시됩니다.
CSCvs56617	캡티브 포털(captive portal)에서 사용자는 원하는 대로 이메일 전송을 트리거할 수 있습니다.
CSCvs58106	NAD CSV 가져오기는 TrustSecDeviceID에서 지원되는 모든 문자를 허용해야 합니다.
CSCvs60518	ISE 관리자 사용자가 내부 사용자의 그룹을 변경할 수 없음
CSCvs62081	반복되는 pxGrid 및 DNAC 메시지로 채워진 수집기 로그
CSCvs62586	Tacacsprofile이 REST API를 사용하여 올바르게 검색되지 않음
CSCvs62597	REST API를 사용하여 Authz 프로파일을 올바르게 가져오지 못함(태그 누락)
CSCvs65467	Cisco ISE(Identity Services Engine) 저장된 사이트 간 스크립팅 취약점
CSCvs65989	네트워크 디바이스/그룹을 가져온 후 새 위치를 추가할 수 없음
CSCvs67042	ISE 2.2 이상은 메모리 누수의 영향을 받습니다. Inflater()로 인해 기본 메모리에서 매일 1~2% 증가
CSCvs68914	ERS API를 통해 밑줄로 Security Group(보안 그룹)을 생성하면, ISE 오류 발생
CSCvs69726	ISE 2.2 이상은 메모리 누수의 영향을 받습니다. 기본 메모리가 매일 PORT_Alloc_Util() 1~2% 증가

고지 ID 번호	설명
CSCvs70997	ISE: SCEP RA를 구성할 때, 2.4p9 Intermediate CA(중간 CA)가 설치되지 않음
CSCvs75068	오류가 발생하여 % 또는 <을(를) 포함하는 레지스트리 키 값 조건을 추가할 수 없음
CSCvs75274	"Certificate Provisioning Portal(인증서 프로비저닝 포털)"에 대한 포털 사용자 맞춤화를 수행할 수 없습니다.
CSCvs76257	RadiusProxyFlow::stripUserName()에서 사용자 이름 대신 빈 문자열로 인해 ISE가 충돌함
CSCvs77182	ISE: HTTPS에서 "url-redirect" 속성을 사용할 수 없습니다. HTTP가 있는 동일한 URL이 정상적으로 작동합니다.
CSCvs78160	INetworkAuthZCheck의 ConditionsData 절에서 URT 실패
CSCvs79836	만료된 인증서가 삭제되지 않음
CSCvs82557	SXP 바인딩이 pxGrid 2.0 클라이언트에 게시되지 않음
CSCvs83303	임시 업데이트가 DB에 저장되지 않은 경우, API에서 데이터를 검색하지 않음
CSCvs85970	AD join-point에 'TACACS' 문자열이 있으면, AuthZ 조건에서 AD joinpoint가 표시되지 않음
CSCvs86344	게스트 사용자 이름에 @ 기호(guest@example.com)가 포함되어 있으면, ISE 2.4 Guest ERS Call Get-By-Name이 실패함
CSCvs86775	ISE 2.6 설치: 입력 검증-IP 도메인 이름 확인
CSCvs88368	해시 비밀번호를 사용할 때, ISE SNMP 서버가 충돌합니다.
CSCvs89440	PAN 전용 노드에 대해 CEPM 스키마 통계가 수집/예약되지 않음
CSCvs89683	ADE-OS 로그에 일반 텍스트로 인쇄된 BunnyMQ 사용자 비밀번호를 마스크 처리하거나 제거해야 함
CSCvs91026	Docker image ise-rabbitmq를 성공적으로 로드한 후 컨피그레이션을 재설정할 수 없음
CSCvs91408	LONG: 수명(Longevity) 테스트의 PMNT 노드에서 상당한 메모리 증가
CSCvs91808	특수 문자가 포함된 메타 데이터 xml 파일을 가져오면 지원되지 않는 태그 오류가 발생함
CSCvs96516	여러 Cisco ISE(Identity Services Engine)에 저장된 사이트 간 스크립팅 취약점
CSCvs96541	OP 백업을 복원한 후 TACACS auth/acc 보고서가 표시되지 않음

고지 ID 번호	설명
CSCvs96544	CV 2.4 패치 9로 엔드포인트 CSV 파일을 가져오면, '설명' 필드가 유지되지 않음
CSCvs96560	많은 수의 엔드포인트가 있는 경우, ISE ERS API 조회 속도가 느림
CSCvs97302	.dmp 파일은 ISE에서 reset-config 이후에도 /opt/oracle/base/admin/cpm10/dpdump에서 삭제되지 않음
CSCvs98094	ISE 2.7 서버에서 테스트하는 동안, 파일 교정 확인이 실패함
CSCvt00283	게스트가 후원하는 포털의 성공 페이지를 새로 고치면, 404 오류 발생
CSCvt00780	BYOD 시작 페이지에서 OS 탐지 메시지에 대한 메시지를 현지화할 수 없음
CSCvt01161	NMAP-MCAFeeEPROOrchestratorClientscan이 ISE 2.6버전에서 실행되지 않음
CSCvt03094	ISE 만료 TACACS 세션이 세션 캐시에서 적시에 지워지지 않음
CSCvt03292	인증서 취소 및 CPP가 APEX 라이선스 없이 작동하지 않습니다.
CSCvt03935	TrustSec Policy Matrix--ISE에서 "View(보기)" 옵션 표현 변경
CSCvt04047	POST getBackupRestoreStatus는 백업/복원 메뉴로 이동한 후 모든 ISE 페이지에서 발생
CSCvt04144	Alarm Settings(알람 설정)에서 높은 디스크 사용률에 대한 임계값 옵션 없음
CSCvt05201	터널 그룹 정책 평가를 사용하는 포스처에서 Java Mem 사용 중단
CSCvt07230	ISE는 가져올 때 이 Egress Policy(이그레스 정책)에서 어떤 것도 허용해서는 안 됩니다.
CSCvt08143	ISE 2.6의 시간 차이
CSCvt09164	ISE 2.2 P16 이미 확장 게스트 사용자를 다시 확장할 수 없음
CSCvt09434	SCCM 서버 시간 초과를 처리하기 위해 적절한 로깅 및 보고 추가
CSCvt09458	ISE MDM 통합-디버그에서 잘못된 COA 유형
CSCvt10214	[ENH] 네트워크 디바이스용 API를 사용하여 "GET|PUT|DELETE by Name"에 기능 추가
CSCvt11130	Sh 버전 명령이 유효한 ISE 비관리자 CLI 사용자가 아님
CSCvt11179	AD 서버에서 이 OS 속성이 변경될 때 "AD-Operating-System" 속성을 가져오지 않음
CSCvt11366	CLI에서 엔드포인트를 내보내면, java 예외가 발생함

고지 ID 번호	설명
CSCvt11380	DNAC가 GBAC를 관리하는 경우에도 Policy Sets(정책 집합) 이벤트 내에서 SGT를 생성할 수 있음
CSCvt11664	'createLicenseSource' 메서드 "FlexlmListException: Error"를 통해 ISE 피드 서버 실패
CSCvt12236	IP SGT 정적 매핑 가져오기가 호스트네임과 올바르게 작동하지 않음
CSCvt13707	pxGrid 2.0 WebSocket 분산 업스트림 연결 문제
CSCvt13719	유휴 독립형에서도 pxGrid 2.0 WebSocket ping pong이 너무 느림
CSCvt13746	Authz 정책 및 예외가 더 있는 경우, ISE에 모든 디바이스 관리자 권한 규칙이 표시되지 않음
CSCvt14248	ISE 2.6/2.7로 업그레이드한 후, EST 서비스를 초기화하는 Certificate Authority 서비스가 실행되지 않음
CSCvt15256	"Guest user(게스트 사용자)" ID 저장소가 사용되면, 인증이 처리되지 않습니다.
CSCvt15893	예방 버그: ISE2.6으로 업그레이드한 후, Radius 오류/잘못 구성된 신청자 테이블이 존재하지 않음
CSCvt15935	일부 노드에 대해 System Summary Dashboard(시스템 요약 대시보드)와 일치하는 높은 로드 알람이 채워지지 않음
CSCvt16882	Apple CNA 및 AUP를 링크로 사용하여 iPad에서 포털에 액세스하는 경우, 400 Bad Request(잘못된 요청) 오류가 발생합니다.
CSCvt17283	AVC를 활성화하는 동안, GUI 속도 저하
CSCvt17783	ISE는 SGT 가져오기 또는 내보내기를 통해 모든 SGT 또는 값 65535가 노출되지 않도록 해야 함
CSCvt18613	AD 그룹이 있는 AuthZ 조건이 TEAP에 대해 일치하지 않음-EAP-Chaining
CSCvt19657	많은 수의 엔드포인트가 있는 경우, ISE ERS API 엔드포인트 업데이트 속도가 느림
CSCvt22900	"*Endpoint Consumption Count Updated:"가 라이선싱에서 업데이트되지 않음
CSCvt24276	시스템 사용 사전에 6개가 넘는 속성을 허용/추가할 수 없음
CSCvt25610	ISE2.7 컴플라이언스 카운터가 0임
CSCvt26108	ISE 2.7 AnyConnect 컨피그레이션의 보류 업데이트가 저장되지 않음
CSCvt34876	RADIUS 및 높은 CPU에 대응하는 ISE 레이턴시

고지 ID 번호	설명
CSCvt35044	EP 조회에 더 많은 시간이 소요되어 게스트 플로우의 레이턴시가 길어짐
CSCvt35239	clientMac이 null일 때 포스처 플로우 중에 catalina.out에서 NullpointerException이 발생함
CSCvt36117	ERS를 통해 ISE의 내부 사용자에 대한 ID 그룹 업데이트
CSCvt36322	URL에 리디렉션 값이 있으면, ISE 2.6 MDM 플로가 실패함
CSCvt36452	ISE에서 평가 프로파일러 라이선스가 만료되면, 기본 반경 프로브가 활성화됨
CSCvt37910	[ENH] /ers/config/internaluser용 API를 사용하여 "GET|PUT|DELETE by Name" 기능 추가
CSCvt38308	ISE: min pwd length가 증가하면, 더 짧은 pwd가 있는 경우에 오류 없이 GUI를 통해 로그인하지 못함
CSCvt40534	MNT 노드 선택 프로세스가 제대로 설계되지 않았습니다.
CSCvt42064	ISE가 포스처 세션 조회 호출을 SSH 로그인으로 잘못 보고함
CSCvt43844	ISE: runtime-aaa 디버그는 패킷 상세정보를 ASCII로 인쇄하지 않음, 엔드포인트 디버그 중단
CSCvt46584	디스크 공간 문제로 인한 백업 실패가 제거되지 않음 ENDPOINTS_REJECT_RELEASE 테이블
CSCvt46850	조건 라이브러리를 사용하여 저장된 복합 조건을 편집할 수 없습니다.
CSCvt49961	FQDN으로 구성된 Syslog Target(Syslog 대상)으로 인해, Network Outage(네트워크 중단)이 발생할 수 있음
CSCvt53541	SMS over HTTPS가 사용자 이름/비밀번호를 게이트웨이로 전송하지 않음
CSCvt55300	redis의 IP 속성이 제거된 경우에도 "Current IP address" CV에 표시됩니다.
CSCvt55312	Apple CNA의 ISE BYOD가 9800으로 실패함
CSCvt57274	어제와 오늘에 대한 Authentication Summary Report(인증 요약 보고서)에 데이터가 표시되지 않음
CSCvt57571	IP 액세스가 항목 없이 제출되면, 앱 서버가 충돌함
CSCvt57805	REST API 업데이트 작업에 대한 간헐적인 비밀번호 규칙 오류
CSCvt61181	ISE ERS API-SNMP 컨피그레이션을 처리하는 동안, 네트워크 디바이스에서 GET 호출이 느림

고지 ID 번호	설명
CSCvt63793	포스처-LSD를 사용하지 않는 경우, "No policy server detected (탐지된 정책 서버 없음)"와 함께 비 리디렉션 플로가 실패함
CSCvt65332	두 줄을 사용한 설명 또는 <Enter> 사용됨, Client Provisioning(클라이언트 프로비저닝) 리소스에서 오류 발생
CSCvt65719	잘못된 Null 포인터 예외, 사후 수동 동기화가 수행됨
CSCvt65853	ISE-2.x || 분산형 구축에서 사용할 때 ReAuth에 대한 MNT REST API 실패
CSCvt67595	사용자 인증 실패에 대한 라이브 로그가 표시되지 않음
CSCvt69912	ISE가 여전히 오탐 경보 "Alarms: Patch Failure"를 생성합니다.
CSCvt70689	MAR 캐시 복제가 활성화된 경우, 애플리케이션 서버가 충돌할 수 있음
CSCvt71355	pxGrid가 INIT 상태의 사용자를 삭제할 수 없음
CSCvt71559	알람 대시 렛에 'No Data Found'가 표시됩니다.
CSCvt73953	CLI 내보내기와 Context Visibility(상황 가시성) 사이의 정보가 일치하지 않음
CSCvt76509	SFTP 리포지토리에 공간이 없지만, ISE Backup File(백업 파일) 전송 로그에 성공이 표시됨
CSCvt80285	정의할 안티멀웨어 조건을 생성할 때, 45개 이상의 제품을 선택할 수 없음
CSCvt81194	CPU 스파이크가 HitCountCollector 정책에서 관찰되고 있음
CSCvt82384	diagnostics.log의 회전이 ISE에서 작동하지 않음
CSCvt85722	작동하지 않는 MNT 위젯에 대한 디버그 로그 없음
CSCvt85757	영어가 아닌 문자에 대한 스폰서 포털 표시?
CSCvt85836	세션 캐시가 불완전한 세션으로 채워짐
CSCvt87409	ISE DACL 구문 검사에서 IPv4 형식 오류를 탐지하지 않음
CSCvt89098	ISE가 실패한 노드에 대해 와일드 카드 복제를 재시도하지 않음
CSCvt91871	ISE RADIUS Accounting Repor(ISE RADIUS 어카운팅 보고서) 상세정보에서는 Accounting Details(어카운팅 상세정보) 아래에 "No data found"가 표시됨
CSCvt93117	ise-psc.log가 "check TTConnection is valid"로 가득 차 관련 로그가 롤오버됨
CSCvt93603	ISE 2.6p6 사용자 지정 엔드포인트 속성을 삭제할 수 없음
CSCvt96594	ISE 2.6: ERS를 통해 외부 스폰서 사용자를 사용하여 Guest user(게스트 사용자) 생성에 401 Unauthorized 오류 발생

고지 ID 번호	설명
CSCvu04874	io.netty.buffer.PoolChunk에서 의심되는 메모리 누수
CSCvu05164	ISE가 API를 통해 NAD에서 Radius를 비활성화할 수 없음
CSCvu10009	Internal Users(내부 사용자)와 함께 Update-By-Name 방법을 사용할 경우의 필수 값
CSCvu15948	TC-NAC 어댑터가 Nexpose(insiteVM)로 스캔을 중지함
CSCvu16067	TCP 지연, TACACS 레이턴시를 유발하는 IP-TABLES ISE 2.6의 변경 사항
CSCvu20359	파일 이름에 점(.)이 포함된 파일 확인 조건을 사용할 때, 마크업 언어 오류가 발생함
CSCvu21093	ISE 2.6p6 // 포털 배경이 잘못 표시됨
CSCvu25625	ISE가 DNAC에서 나머지 API 호출에 대해 잘못된 버전을 반환함
CSCvu25975	Tacacs 명령 집합에서 가져오기 옵션이 작동하지 않음
CSCvu28305	ISE 로깅 타임 스탬프에 미래 날짜 표시
CSCvu29434	SNS 3655 PSN에서 다시로드한 후 ISE2.6P6 서비스가 초기화되지 않음
CSCvu30286	다중 매트릭스에서 단일 매트릭스로 이동한 후 ERS SGT 생성이 허용되지 않음
CSCvu31176	2.4P11 VPN + Posture: Apex 라이선스가 사용되지 않음,
CSCvu31853	ERS를 통해 추가된 NDG가 DB의 모든 네트워크 디바이스와 연결됨
CSCvu32240	internaluser 업데이트를 위해 ISR ERS API를 실행할 때, 기존 identityGroups 값이 null로 설정됨
CSCvu32865	ISE 2.7의 높은 CPU가 인증 레이턴시를 유발함
CSCvu33416	유효한 라이선스가 있는 라이선스가 컴플라이언스 위반 알람
CSCvu33861	ISE 2.4 p6-MAC 주소별로 디바이스를 가져오는 REST API MnT 쿼리에 2초 이상 소요됨
CSCvu34433	ISE 2.x, 실행 취소 테이블 스페이스의 여유 공간이 isehourlycron.sh cron 스크립트에 따라 지워지지 않음
CSCvu34895	보고서 리포지토리 내보내기가 전용 MNT 활성화에서 작동하지 않습니다.
CSCvu35802	Shared email for AD 사용자가 그룹을 검색하지 못함, ISE가 포리스트에 있는 여러 계정을 표시함
CSCvu39653	MAC 주소에 대한 세션 API가 허용되는 범위를 벗어난 Char 0x0을 반환함

고지 ID 번호	설명
CSCvu41815	[CFD] AuthZ 프로파일이 diff SG에 대해 동일한 VN에 매핑되는 경우, SG에서 VN을 삭제하면 GBAC 동기화가 중단됨
CSCvu42244	EAP-TLS를 통한 Machine Authentications(머신 인증)에서 사용자를 찾을 수 없음 오류를 표시하는 권한 부여 플로우 중에 실패
CSCvu47395	ISE 2.x, 3.x: 메모리 문제가 많은 시스템에 Drop_Cache 필요
CSCvu48417	ISE ERS API DELETE 디바이스에서 1 회 이상의 호출로 500 오류 반환
CSCvu49019	Elastic Search(탄력적 검색)에서 의심되는 메모리 유출
CSCvu49724	DNAC에 SNMP v2c 버전이 구성된 디바이스가 ISE의 네트워크 디바이스에 표시되지 않음
CSCvu53022	ISE: Account OU(어카운트 OU)를 변경한 후 캐시된 AD OU가 새 OU보다 우선함
CSCvu53836	ISE Authorize-Only 요청은 Internal User Groups(내부 사용자 그룹)에 대해 평가되지 않음
CSCvu55332	REST API 호출은 Policy Set(정책 집합)에서 참조되는 Network Device Group(네트워크 디바이스 그룹)을 제거할 수 있음
CSCvu55557	REST API를 사용하여 NAD를 생성하는 경우, Radius secret 4 자 최소 요구 사항이 확인되지 않음
CSCvu58476	ID 저장소에 문제가 있을 때, My Device Portal(내 디바이스 포털)에서 오류 메시지 개선
CSCvu58793	위치 기준 필터를 사용할 때, ERS REST API에서 중복값을 여러 번 반환함
CSCvu59093	SessionDB 열이 ISE에서 누락됨(>=2.4)
CSCvu59491	ISE가 insiteVM(tc-nac 서버)에 새 사이트 생성
CSCvu63642	Context Visibility(상황 가시성)이 사용자 이름 업데이트 시 엔드포인트 매개변수를 통합함
CSCvu63833	AD가 ID 소스로 선택되는 경우, Audit Report(감사 보고서)에 Failed Logins to ISE GUI(ISE GUI에 대한 실패한 로그인)이 표시되지 않음
CSCvu67707	CWE-937 알려진 취약점이 포함된 JavaScript 라이브러리 사용
CSCvu68700	잘못된 크레덴셜이 있는 XML 또는 JSON 요청에 대한 ISE 2.6 p5 ERS API 해상도가 HTTP 401이며, 예기치 않은 HTML 본문이 있음
CSCvu70683	iselocalstore.log에서 억제와 함께, ERS 쿼리에 대한 알람 억제 필요

고지 ID 번호	설명
CSCvu70768	경보 및 시스템 요약이 ISE GUI에 표시되지 않음
CSCvu73387	인증 실패, 이유: "12308 Client sent Result TLV indicating failure"
CSCvu74198	ISE: LDAP 및 ODBC ID 저장소 이름에 하이픈이 허용되지 않음
CSCvu83759	sftp 리포지토리에서 변경 사항을 확인한 후, ISE가 키 쌍을 삭제함
CSCvu90107	ISE는 모든 버전의 ERS 플로우에서 중복 디바이스 ID를 허용합니다.
CSCvu90703	CLDAP 스레드가 중단되고 무한대로 실행됨
CSCvu91016	ATZ 정책의 InternalUser 속성에서 TACACS+ ASCII 인증 실패
CSCvu91601	ISE Authentication Status(인증 상태) API 호출 기간이 예상대로 작동하지 않음
CSCvu94733	잘못된 비밀번호에 대해 "Account is not yet active"로 게스트 인증이 실패함
CSCvv00377	서브넷 및 IP 범위를 사용하는 네트워크 디바이스 중복
CSCvv070490.	ISE가 포트 번호를 사용하여 ODBC "Connection failed"에 연결할 수 없음
CSCvv09167	TACACS 집계 테이블이 제대로 제거되지 않았습니다.
CSCvv15811	IP 주소가 할당된 종료 인터페이스가 있는 경우, ISE TCP 포트 84xx가 열리지 않음
CSCvv23256	ISE Authentication Status(인증 상태) API 호출이 지정된 시간 범위에 대한 모든 레코드를 반환하지는 않음
CSCvv26811	Policy Export(정책 내보내기)가 암호화로 저장된 후에는 암호화 없이 저장되지 않음
CSCvv44914	isedataupgrade.sh가 실패했습니다. ISE 전역 데이터 업그레이드 실패-ISE 2.6P6에서 -2.7,3.0

Cisco ISE 릴리스 3.0의 미결 경고(Open Caveats)

고지 ID 번호	설명
CSCvq75448	많은 수의 SGT로 인해, ISE에 대한 FMC 구독을 사용할 수 없음
CSCvr24059	소스 SGT 상관관계가 FMC 및 FTD 6.5에서 작동하지 않음
CSCvv45728	ISE Admin GUI의 일부 레이블이 일본어로 변환되지 않음
CSCvv54305	"Support TrustSec Verification reports(지원 TrustSec 확인 보고서)" 확인란을 활성화하면 안 됩니다.

고지 **ID** 번호	설명
CSCvv54754	IE 최신 버전: Portal 타일이 DB 복원 설정의 게스트 포털 페이지에서 중복됩니다.
CSCvv55971	IE GUI: 진행률 표시줄 및 정보 아이콘이 상태 확인 페이지의 모듈 이름과 겹치거나 잘못 정렬되었습니다.
CSCvv57822	TRACE 레벨 디버그로 인한 pxgrid 노드의 교착 상태.
CSCvv58353	HTTPS ServerList config가 2.7 P1에서 ISE 3.0으로 지속적으로 업그레이드하지 않음
CSCvt97146	[ISE-3.0] WSA에서 지속적으로 충돌하는 ISED
CSCvu78668	[ISE3.0]: 세션이 없으면 ISE-WSA 통합 실패
CSCvv66302	도메인이 SXP 피어에 할당되지 않음
CSCvv67101	TAC 지원 케이스 리디렉션 문제

통신, 서비스 및 추가 정보

- Cisco에서 시기에 맞는 관련된 정보를 받으려면, Cisco Profile Manager(Cisco 프로파일 관리자)에 로그인합니다.
- 중요한 기술로 원하는 비즈니스 결과를 얻으려면, Cisco Services(Cisco 서비스)를 참조하십시오.
- 서비스 요청을 제출하려면, Cisco Support(Cisco 지원)을 참조하십시오.
- 안전하고 검증된 엔터프라이즈급 앱, 제품, 솔루션 및 서비스를 검색하고 찾아보려면, Cisco Marketplace(Cisco 마켓플레이스)를 참조하십시오.
- 일반 네트워킹, 교육 및 인증서 제목을 얻으려면, Cisco Press(Cisco 프레스)를 참조하십시오.
- 특정 제품 또는 제품군에 대한 보증 정보를 찾으려면, Cisco Warranty Finder(Cisco 보증 찾기)에 액세스합니다.