

Cisco ISE(Identity Services Engine)

Cisco® ISE(Identity Services Engine)를 사용하면 기업 네트워크에 연결하는 사용자 및 디바이스를 보고 제어할 수 있습니다. 이 모든 작업은 중앙 위치에서 수행됩니다.

제품 개요

진화하는 모바일 엔터프라이즈의 관리하고 보안을 유지하려면 색다른 접근 방식이 필요합니다. Cisco ISE는 탁월한 사용자 및 디바이스 가시성을 통해 기업에 간소화된 모빌리티 경험을 제공합니다. 또한 중요한 상황 데이터를 통합 기술 파트너 솔루션과 공유합니다. Cisco ISE가 제공하는 통합, 합병, 자동화를 통해 위협을 더 빠르게 식별, 억제 및 치료할 수 있습니다.

고객 혜택

Cisco ISE는 네트워크 액세스 보안에 대한 종합적인 접근 방식을 제공합니다. Cisco ISE가 구축되면 다음과 같은 여러 이점을 누릴 수 있습니다.

회사 정책에 따른 **비즈니스 보호 및 상황 정보 기반 액세스**. ISE로 사용자, 엔드포인트 및 기타 특성(예: 시간, 위치, 액세스 유형 또는 방법)을 일치시키고 모든 것을 포괄하는 상황별 ID를 생성할 수 있습니다. 이러한 ID는 해당 ID의 비즈니스 역할과 일치하는 보안 액세스 정책을 시행하는 데 사용됩니다. IT 관리자는 네트워크에서 허용되는 사용자 및 작업을 정확하게 제어할 수 있습니다. IT 관리자는 소프트웨어 정의 세그멘테이션을 지원하는 [Cisco TrustSec®](#) 솔루션 등의 여러 가지 메커니즘을 사용하여 정책을 시행합니다.

간편하고 유연하며 쉽게 사용할 수 있는 인터페이스를 통한 **간소화된 네트워크 가시성**. 이제 ISE에서 연관된 가시성을 통해 네트워크에 있었던 모든 엔드포인트의 기록을 저장할 수 있습니다. 그리고 간소화된 가시성 마법사를 통해 가치 증명을 신속하게 설정하여 현재 네트워크에 있는 모든 엔드포인트의 가시성을 입증할 수 있습니다.

끊임없이 변화하는 비즈니스 요구를 충족시킬 수 있도록 액세스 규칙을 쉽고 유연하게 정의할 수 있는 **확장된 정책을 시행**. 전체 네트워크 및 보안 인프라 전반에 정책 시행을 분산하는 중앙 집중화된 위치에서 이러한 작업을 수행할 수 있습니다. IT 관리자는 게스트 사용자 및 디바이스를 등록된 사용자 및 디바이스와 구분하는 정책을 중앙에서 정의할 수 있습니다. 액세스 위치에 상관없이 해당 상황에 따라 사용자 및 엔드포인트의 액세스가 허용됩니다.

네트워크에 다양한 레벨의 액세스를 제공하는 **간소화된 게스트 환경**. 게스트는 커피숍의 핫스팟이나 셀프 서비스 등록 액세스 또는 스폰서 액세스를 사용하여 특정 리소스에 액세스할 수 있습니다. 동적 시각형 톨은 사용자가 경험하는 포털 화면 및 단계에 대한 실시간 미리보기를 제공합니다. 변경 사항이 스폰서 게스트 어카운트, 셀프 등록, SMS, 액세스 이메일 확인 관련 설정에 어떤 영향을 미치는지 볼 수 있습니다. [ISE 무선 게스트 설정 가이드](#)를 사용하면 구축이 쉽고 빨라집니다.

기업의 BYOD(Bring-Your-Own-Device) 또는 게스트 정책을 구현하기 위한 **셀프 서비스 디바이스 온보딩**. 사용자는 IT 관리자가 정의한 비즈니스 정책에 따라 디바이스를 관리할 수 있습니다. IT 직원은 보안 정책 준수에 필요한 디바이스 프로비저닝, 프로파일 구축 및 상태 확인을 자동화할 수 있습니다. 동시에, 직원은 IT 지원 없이 네트워크에 자신의 디바이스를 연결할 수 있습니다.

모든 기업 네트워크 전반에 걸쳐 정책 생성, 가시성, 보고가 간소화된 **단일 관리 콘솔**. IT 직원은 감사, 규정 요건, IEEE 802.1X 표준에 대한 필수 연방 지침을 쉽게 검증할 수 있습니다.

Cisco AnyConnect® Unified Agent를 이용하여 디바이스 상태 확인 및 치료 옵션을 지원하는 **자동 디바이스 컴플라이언스 검사**. AnyConnect® 에이전트는 데스크톱 및 노트북 컴퓨터 확인을 위한 고급 VPN 서비스도 제공합니다. ISE를 업계 최고의 MDM/EMM(Mobile Device Management/Enterprise Mobility Management) 벤더와 통합할 수도 있습니다. 이러한 통합을 통해 모바일 디바이스가 충분히 안전하고 정책을 준수하는지 확인한 후 네트워크 액세스 권한을 부여할 수 있습니다.

네트워크 전반에 대한 동적 상황 데이터를 구성하는 **사용자 및 디바이스 세부 정보 공유**. Cisco **pxGrid 기술**은 연결된 사용자 및 디바이스에 대한 더욱 심층적인 상황 데이터를 Cisco 및 Cisco **기술 파트너 솔루션**과 공유할 수 있는 강력한 플랫폼입니다. ISE 네트워크 및 보안 파트너는 이러한 데이터를 사용하여 자체 네트워크 액세스 기능을 개선하고 네트워크 위협을 식별, 완화, 치료하는 솔루션 기능의 속도를 높일 수 있습니다.

MDM/EMM 벤더, SIEM(Security Information and Event Management), 위협 방어를 위한 기술 파트너를 포함하고 있는 **기술 파트너 커뮤니티에 액세스** 가능.

제품 기능 및 장점

Cisco ISE는 여러 가지 방법으로 조직의 역량을 높여줍니다(표 1).

표 1. 기능 및 장점

기능	장점
중앙 집중식 관리	<ul style="list-style-type: none"> 관리자가 프로파일러, 상태, 게스트, 인증 및 권한 부여 서비스를 단일 웹 기반 GUI 콘솔에서 중앙 집중식으로 구성하고 관리할 수 있도록 지원합니다. 단일 창에서 통합된 관리 서비스를 제공함으로써 관리를 간소화합니다.
비즈니스 정책 시행	<ul style="list-style-type: none"> 규칙을 기반으로 하는 특성 중심의 정책 모델을 제공하여, 유연하면서도 비즈니스에 적합한 액세스 제어 정책을 지원합니다. 또한 미리 정의된 사전에서 특성을 가져와 세분화된 정책을 만들 수 있습니다. 이러한 특성에는 사용자 및 엔드포인트 ID, PV(Posture Validation), 인증 프로토콜, 프로파일 구축 ID 및 기타 외부 특성 소스가 포함됩니다. 특성은 동적인 방식으로 생성해 저장해 두었다가 나중에 사용하는 것도 가능합니다. Microsoft Active Directory, LDAP(Lightweight Directory Access Protocol), RADIUS, RSA OTP(One-Time Password), 인증 및 권한 부여에 대한 인증서 권한 같은 여러 가지 외부 ID 저장소와 통합하며 ODBC(Open Database Connectivity)를 지원합니다.
액세스 제어	<ul style="list-style-type: none"> dACL(downloadable Access Control Lists), VLAN 할당, URL 리디렉션, 명명된 ACL, Cisco TrustSec 기술 지원 네트워크 디바이스의 고급 기능을 사용하는 SGT(Security Group Tag)를 포함하여 광범위한 액세스 제어 옵션을 제공합니다.
EasyConnect를 통해 보안이 뛰어난 무선 네트워크 액세스 지원	<ul style="list-style-type: none"> 인증 및 권한 부여를 위해 엔드포인트를 구성하지 않고도 보안이 뛰어난 네트워크 액세스를 신속하게 돌아올 수 있는 기능을 제공합니다. 애플리케이션 레이어를 통해 로그인 정보에서 인증 및 권한 부여 정보를 얻어 엔드포인트에 802.1x 서플리컨트(supplicant) 없이도 사용자 액세스가 허용됩니다.
SXP(Source-Group Tag Exchange Protocol) 지원	<ul style="list-style-type: none"> SXP(Source-Group Tag Exchange Protocol) 초안에 정의된 대로 SXP 스피커 또는 리스너로서의 역할을 수행하고, SGT(Source-Group Tag) 정보에 대한 네트워크의 소스 저장소(Source of Truth) 역할을 수행할 수 있습니다. 전체 네트워크에 걸쳐 차별화된 역할 기반 액세스를 제공하기 위해 Cisco TrustSec 정책을 준수하지 않는 세그먼트들을 브리지로 연결합니다.

기능	장점
게스트 액세스 기간 관리	<ul style="list-style-type: none"> • 게스트 네트워크 액세스를 구현하고 맞춤화하기에 적합한 간소화된 경험을 제공합니다. • 광고 및 프로모션을 통해 몇 분 만에 기업 브랜드의 게스트 환경을 생성할 수 있습니다. 핫스팟, 스폰서, 셸프 서비스 지원이 내장되어 있으며 및 다양한 액세스 워크플로우를 지원합니다. • 관리자에게 게스트 플로우 설계 효과를 실제로 보여주는 실시간 시각 플로우를 제공합니다. • 보안 및 컴플라이언스 요구 사항, 완전한 게스트 감사를 위해 네트워크 전반에 걸쳐 액세스를 추적합니다. 시간 제한, 어카운트 만료, SMS 인증을 통해 추가적 보안 제어가 가능합니다.
간소화된 디바이스 온보딩	<ul style="list-style-type: none"> • 표준 PC 및 모바일 컴퓨팅 플랫폼에 대한 자동 서플리컨트(suppliment) 프로비저닝 및 인증서 등록을 제공합니다. 이를 통해 IT 헬프 데스크 사례가 감소하며 사용자에게는 더 나은 경험과 더욱 안전한 액세스가 제공됩니다. • 최종 사용자는 셸프 서비스 포털을 사용해 디바이스를 추가 및 관리할 수 있으며 웹 포털용 SAML 2.0을 지원합니다. • MDM/EMM 벤더와 통합하여 모바일 디바이스를 등록하고 액세스 정책을 준수하는지 확인합니다.
내장 AAA 서비스	<ul style="list-style-type: none"> • AAA(Authentication, Authorization, Accounting) 목적으로 표준 RADIUS 프로토콜을 사용합니다. • PAP, MS-CHAP, EAP(Extensible Authentication Protocol)-MD5, PEAP(Protected EAP), EAP-FAST(Flexible Authentication via Secure Tunneling), EAP TLS(Transport Layer Security), EAP-TTLS(Tunneled Transport Layer Security) 외에도 다양한 인증 프로토콜을 지원합니다. 참고: Cisco ISE는 시스템 및 사용자 크리덴셜의 EAP 연결을 지원하는 유일한 RADIUS 서버입니다.
디바이스 관리 액세스 제어 및 감사	<ul style="list-style-type: none"> • TACACS+ 프로토콜을 지원하여 사용자가 TACACS+ 프로토콜을 지원하는 디바이스(예: 네트워크 디바이스 및 서버)에 액세스할 경우 이러한 사용자에 대한 인증, 권한 부여, 감사를 수행할 수 있습니다. • 사용자는 크리덴셜, 소속된 그룹, 연결 위치, 디바이스에서 수행하려는 작업의 종류를 기준으로 모든 디바이스에서 명령에 대한 액세스 권한을 부여받을 수 있습니다. • 네트워크의 모든 변경 사항에 대해 감사 추적을 유지하면서 인가 항목 및 조치에 따라 디바이스 컨피그레이션에 대한 액세스를 제공합니다.
내부 인증 기관	<ul style="list-style-type: none"> • 구축하기 쉬운 내부 인증 기관을 제공하므로 디바이스의 인증서를 간편하게 관리할 수 있습니다. 복잡하게 외부 인증 기관에 신청할 필요가 없습니다. • 단일 콘솔을 사용하여 엔드포인트 및 해당 인증서를 관리할 수 있습니다. 인증서 상태는 표준 기반 OCSP(Online Certificate Status Protocol)를 통해 검사됩니다. 인증서 해지는 자동으로 이루어집니다. • 독립형 구축뿐만 아니라 중속형 구축도 지원합니다. 이는 인증 기관이 기존 엔터프라이즈 PKI(Public Key Infrastructure)와 통합된 것입니다. • 대량 혹은 단일 인증서 및 키 쌍을 수동으로 생성하고 높은 수준의 보안을 이용하여 디바이스를 네트워크에 연결합니다.
디바이스 프로파일 구축	<ul style="list-style-type: none"> • 제품 출하 시 IP 전화, 프린터, IP 카메라, 스마트폰, 태블릿 등 다양한 유형의 엔드포인트를 위해 사전 정의된 디바이스 템플릿이 포함되어 있습니다. • 맞춤형 디바이스 템플릿을 생성하여 엔드포인트가 네트워크에 연결되면 이를 자동 탐지하고 분류한 후 관리자가 정의한 ID와 연결할 수 있습니다. • 디바이스 유형에 따라 엔드포인트별 권한 부여 정책을 연결시킬 수 있습니다. • 패시브 네트워크 모니터링 및 텔레메트리를 통해 엔드포인트 특성 데이터를 수집합니다. Cisco Catalyst® 스위치에 있는 디바이스 센서를 이용하여 실제 엔드포인트나 Cisco 인프라를 쿼리합니다.
디바이스 프로파일 피드 서비스	<ul style="list-style-type: none"> • 여러 벤더의 다양한 IP 지원 디바이스에 대해 Cisco의 검증된 서비스 프로파일을 자동으로 업데이트하는 기능을 제공합니다. 모든 최신 디바이스를 탐지하고 간편하게 이에 대한 최신 정보를 파악합니다. • 이 서비스에서는 파트너와 고객이 직접 사용자 지정한 프로파일 정보를 공유하면 Cisco에서 이를 검사 및 재구축하는 메커니즘도 제공합니다.
엔드포인트 보안 상태 서비스	<ul style="list-style-type: none"> • 네트워크에 연결하는 PC 및 모바일 디바이스에 대한 엔드포인트 보안 상태 평가를 수행합니다. • 지속적인 클라이언트 기반 에이전트, 임시 에이전트 또는 외부 MDM/EMM 벤더 시스템에 대한 쿼리를 통해 엔드포인트가 적절한 컴플라이언스 정책과 부합되는지를 검증합니다. • 최신 OS 패치, 현재 정의의 파일 변수(버전, 날짜 등)가 최신 상태인 안티바이러스 및 안티스파이웨어 패키지, 안티멀웨어 패키지, 레지스트리 설정(키, 값 등), 패치 관리, 디스크 암호화, 모바일 PIN 잠금/루팅/탈옥 상태, 애플리케이션 상태, USB 첨부 미디어에 대한 확인 작업 이외에도 다양하고 강력한 정책 설정 기능을 제공합니다. • 엔드포인트가 회사 정책을 위반하지 않도록 PC 클라이언트의 자동 치료 및 정기 평가 시행과 더불어 업계 최고의 패치 관리 시스템을 지원합니다. • Microsoft Windows 7, 8, 또는 10(32비트 64비트) 및 Mac OS X 10.7, 10.8, 10.9, 10.11 등 OS 플랫폼에 대한 보안 상태를 평가하려면 AnyConnect 4.x 에이전트가 필요합니다.
광범위한 다중 포레스트 Active Directory 지원	<ul style="list-style-type: none"> • 다중 포레스트 Microsoft Active Directory 도메인에 대한 포괄적인 인증 및 권한 부여를 제공합니다. • 여러 분리된 도메인을 논리적 그룹으로 그룹화합니다. 끊임없이 변화하는 비즈니스 환경을 지원하기 위해 복잡한 Active Directory 토폴로지 컨피그레이션이 간소화되었습니다. • 솔루션의 원활한 전환과 통합을 위한 유연한 ID 재작성 규칙을 포함합니다. • Microsoft Active Directory 2003, 2008, 2008R2, 2012, 2012R2를 지원합니다.

기능	장점
Cisco Rapid Threat Containment	<ul style="list-style-type: none"> • 보안 이벤트에 대응하여 네트워크 완화 및 조사 작업을 수행합니다. • Cisco ISE와 다양한 기술 분야의 Cisco 보안 기술 파트너의 솔루션을 통합합니다. • Cisco pxGrid를 사용하며, 이는 여러 가지 보안 톨이 자동으로 서로 실시간 통신을 수행할 수 있도록 지원하는 매우 안정적인 IT 정보 센터로서의 역할을 수행합니다.
모니터링 및 문제 해결	<ul style="list-style-type: none"> • 모니터링, 보고 및 트러블슈팅을 위해 내장 웹 콘솔을 사용되기 때문에 헬프 데스크 및 네트워크 운영자들이 신속하게 문제를 파악하고 해결할 수 있습니다. • 모든 서비스에 대해 강력한 이력 및 실시간 보고를 제공합니다. 모든 활동을 기록하고 네트워크에 연결된 모든 사용자와 엔드포인트의 실시간 대시보드 메트릭을 제공합니다.
인증	<ul style="list-style-type: none"> • FIPS(Federal Information Processing Standard) 140-2, Common Criteria, Unified Capabilities Approved Product List의 요건을 충족합니다. IPv6 또한 지원합니다. • 참고: 일부 릴리스에서는 인증서가 제공되지 않거나 승인 상태가 달라질 수 있습니다. 최신 인증서 및 릴리스는 Global Government Certifications에서 확인할 수 있습니다.

플랫폼 지원 및 호환성

ISE는 [물리적](#) 또는 가상 어플라이언스 형태 중에서 선택 가능합니다. 물리적 및 가상 폼 팩터를 사용하여 대규모 조직을 위한 ISE 클러스터를 만들 수 있으며, 중요 엔터프라이즈 비즈니스 시스템에 필요한 규모, 이중화 및 페일오버를 제공할 수 있습니다.

ISE 가상 어플라이언스는 VMware ESXi 5.x, 6.x 또는 Red Hat 7.x의 KVM에서 지원됩니다. 프로덕션 구축은 현재 물리적 ISE 플랫폼의 컨피그레이션과 동일하거나 그 이상인 하드웨어에서 실행해야 합니다. 프로덕션 서비스를 제공하지 않는 랩 또는 테스트 환경의 경우, 최소 4GB 메모리 및 최소 200GB 하드 드라이브 공간이 제공되는 가상 대상에서 솔루션을 실행할 수 있습니다.

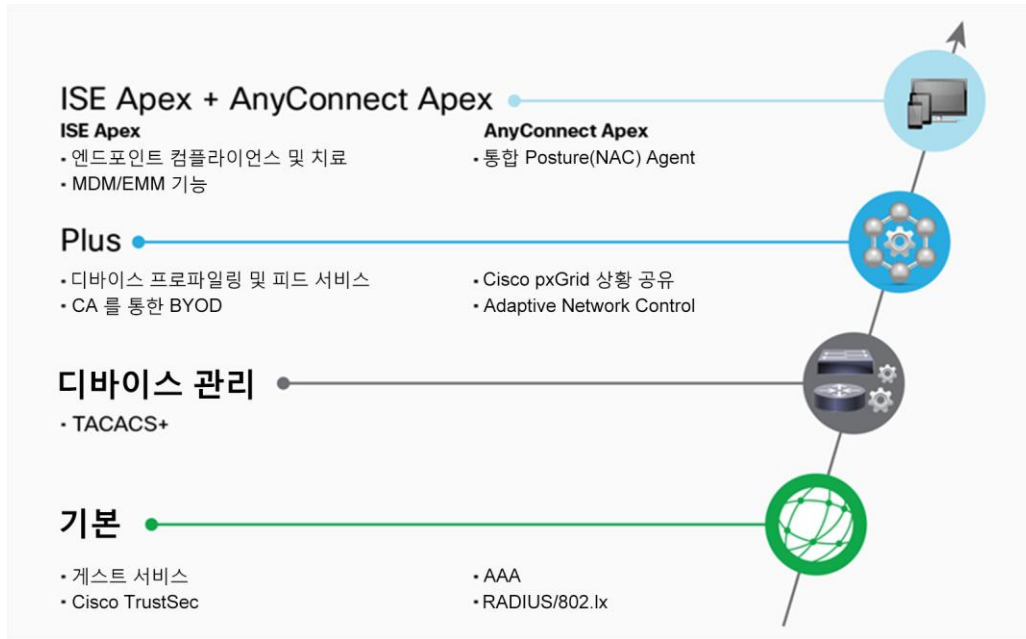
ISE의 물리적 플랫폼 지원에 대한 내용은 [Cisco Secure Network Server Data Sheet](#)를 참조하십시오.

라이선싱 개요

현재 7개의 라이선스 패키지가 제공됩니다(표 1 참조). Base 라이선스에 대한 Cisco 지원 서비스는 Cisco Smart Net Total Care™ Software Application Support plus Upgrades 계약에 따라 달라집니다. 다양한 기간별 라이선스에 대한 Cisco 지원 서비스가 해당 라이선스 기간 동안 지원되는 개별 기간별 라이선스에 포함되어 있습니다.

그림 1에 표시된 것처럼 4개의 주요 ISE 라이선스를 사용할 수 있습니다. 이러한 유연한 모델을 통해 원하는 서비스 세트를 이용하기 위해 라이선스 조합과 수를 선택할 수 있습니다.

그림 1. ISE 라이선스 패키지



주문 정보

Cisco ISE [주문 가이드](#)를 참조하면 서로 다른 모델 및 라이선싱 유형을 이해하는 데 도움이 되며 이를 통해 ISE 구축을 최상으로 활용할 수 있습니다. 제품 주문은 [Cisco 주문 홈페이지](#)를 방문하십시오. ISE 소프트웨어를 다운로드하려면 [Cisco Software Center](#)를 방문하십시오.

서비스 및 지원

Cisco에서는 다양한 서비스 프로그램을 제공하고 있습니다. Cisco의 혁신적인 프로그램은 높은 레벨의 고객 만족을 실현하기 위해 인력, 프로세스, 툴, 파트너의 조합을 통해 제공됩니다. Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. Cisco 서비스에 대한 자세한 내용은 [Cisco Technical Support Services](#) 또는 [Cisco Security Services](#)를 참조하십시오.

워런티 관련 정보는 <http://www.cisco.com/go/warranty>를 참조하십시오. 라이선싱 정보는 <http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-licensing-information-listing.html>을 참조하십시오.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital[®] 금융 지원 솔루션을 통해 여러분이 비즈니스 목표를 달성하는 데 필요한 기술을 도입하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. [자세히 알아보십시오.](#)

추가 정보

Cisco ISE 솔루션에 대한 자세한 내용은 <http://www.cisco.com/go/ise>를 참조하거나 현지 어카운트 담당자에게 문의하십시오.



미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)