CISCO SECURE

# Cisco Secure Client

## 데이터 시트

2022 년 7 월

# Contents


개요 3

Cisco Secure Client 와 AnyConnect 비교 3

알아야 할 중요한 점 4

모듈 및 기능 6

AnyConnect VPN/ZTNA 사용자 및 관리 터널 6

Cisco Secure Endpoint 6

클라우드 관리 모듈 6

Network Visibility Module 6

Umbrella 로밍 보안 모듈 8

ISE Posture 모듈 8

Network Access Manager 8

포스처(Cisco Secure Firewall 용) 8

플랫폼 호환성 15

라이선스 옵션 15

Cisco Capital 15

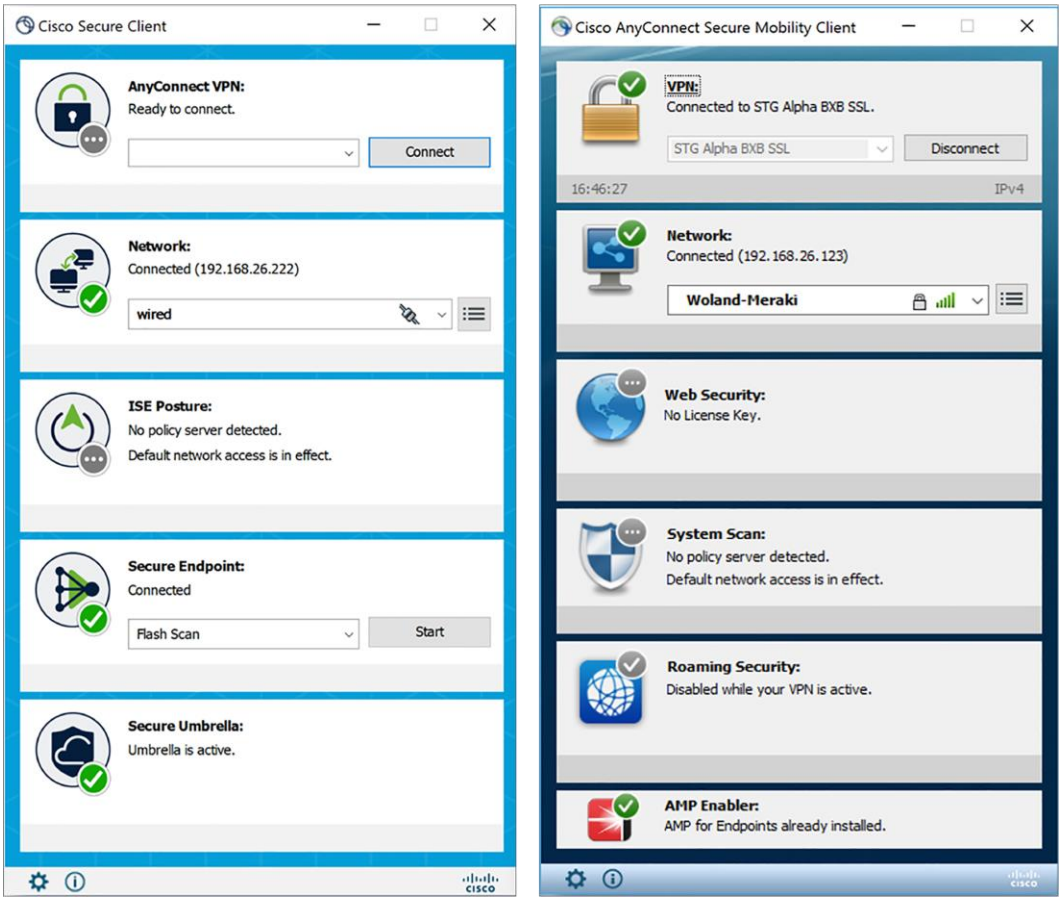
자세히 알아보기 16

## 개요

Cisco Secure Client(이전의 Cisco AnyConnect Secure Mobility Client)는 Windows 10 및 11 에서 사용할 수 있습니다. 일부 브랜딩 및 아이콘을 업데이트한 사용자 인터페이스는 현재 AnyConnect 사용자에게 친숙할 것입니다.

macOS 및 Linux 에서 실행 중인 고객은 Cisco Secure Client 에서 전체 OS 를 지원할 때까지 AnyConnect 4.x 를 계속 활용합니다.

## Cisco Secure Client 와 AnyConnect 비교




Cisco Secure Client 는 가장 널리 구축된 보안 클라이언트 중 하나의 최신 버전입니다. Secure Client 는 원격 액세스 서비스 및 모듈형 보안 서비스 제품군을 제공하는 Cisco AnyConnect 를 기반으로 구축됩니다.

## 알아야 할 중요한 점

AnyConnect 는 이제 Cisco Secure Client 로 알려져 있습니다. 또한 Secure Endpoint(보안 엔드포인트)는 고객에게 통합 고급 EDR(엔드포인트 탐지 및 응답) 및 XDR(확장 탐지 및 응답) 기능을 제공하는 Secure Client 의 새로운 선택적 모듈입니다.

새 사용자는 기존 방법으로 Secure Client 를 설치할 수 있으며, 새로운 클라우드 관리 기능을 도입하려는 고객은 보안 엔드포인트 포털에서 패키지 설치 프로그램을 다운로드하여 설치할 수 있습니다.

디바이스 인사이트가 있는 SecureX 를 통한 클라우드 관리는 Secure Client 의 새로운 선택적 기능입니다. 이 새로운 기능을 사용하면 Secure Client 를 간편하게 구축, 구성 및 모니터링할 수 있습니다. 고객은 클라우드 관리를 채택할 필요가 없으며, 현재 메커니즘을 사용하여 구축을 계속할 수 있습니다. Cisco Secure Firewall, ISE, 소프트웨어 관리 툴(예: SCCM)을 사용하거나 MSI 를 직접 사용합니다.

클라우드 관리를 위한 새로운 SecureX 화면 및 툴은 다음과 같습니다.

- Secure Client 용 네트워크 설치 프로그램 사용자 지정 및 생성
- Secure Client 용 맞춤형 VPN 프로파일 생성 및 다운로드
- 디바이스 인사이트와 통합하여 Secure Client 가 설치된 엔드포인트의 인벤토리 모니터링 및 관리

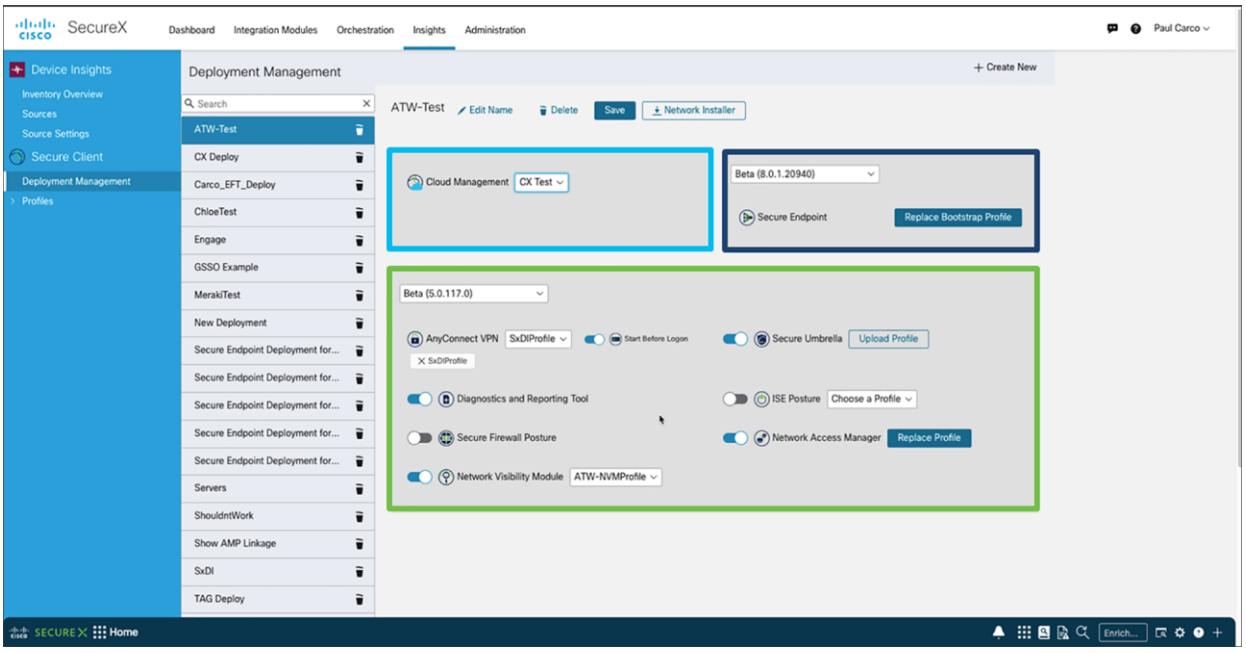



그림 1.
클라우드 관리

## Cisco Secure Endpoint 모듈

### Secure Client 모듈

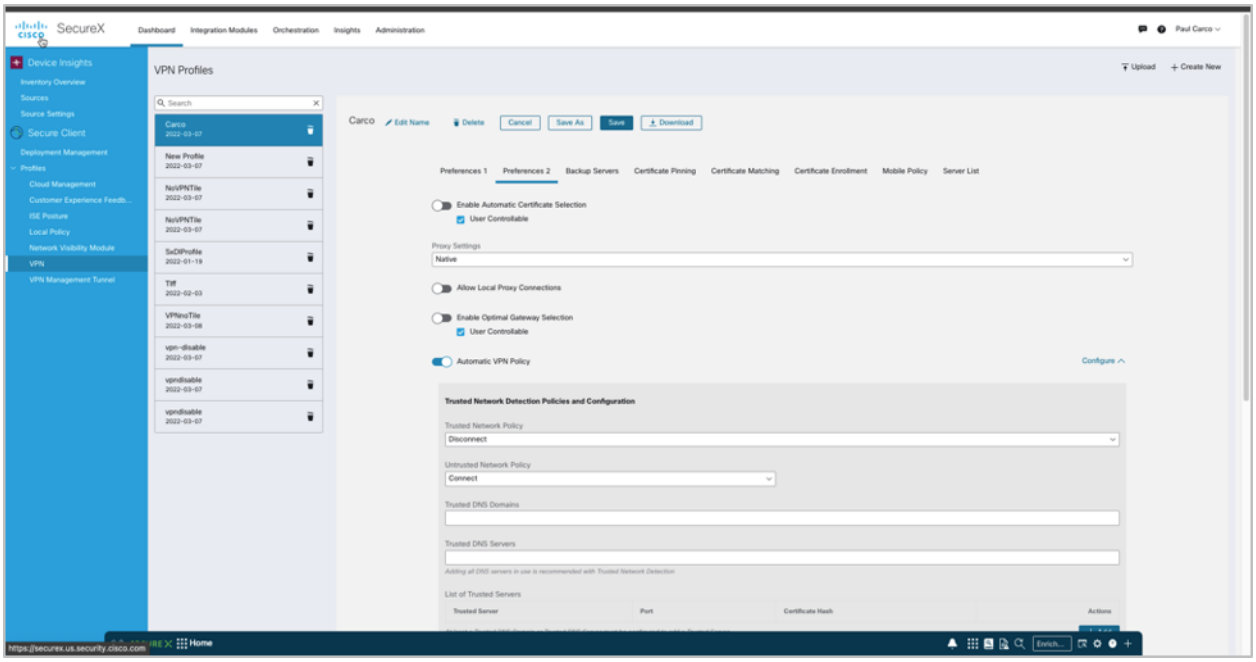



그림 2.
VPN 프로파일

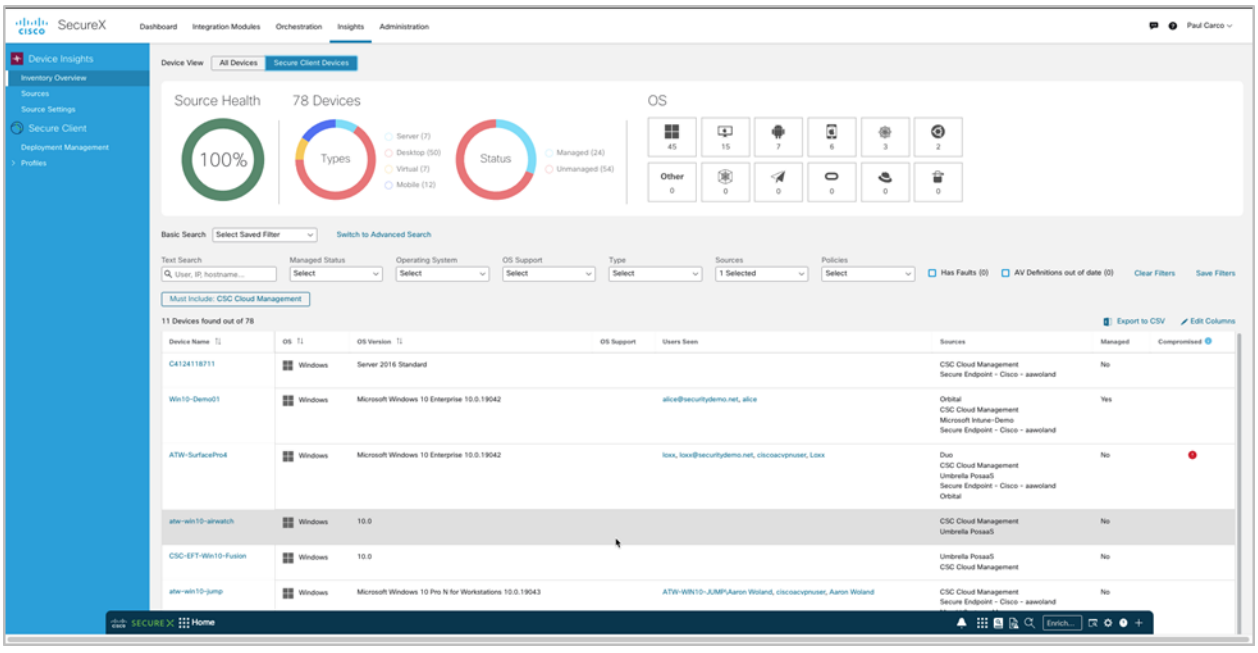



그림 3.
디바이스 인사이트

## 모듈 및 기능

### AnyConnect VPN/ZTNA **사용자 및 관리 터널**

Cisco Secure Client 는 VPN 세션을 자동으로 연결, 다시 연결 또는 연결 해제할 수 있는 여러 옵션을 제공합니다. 이러한 옵션은 사용자에게 VPN 에 연결할 수 있는 편리한 방법을 제공하고 네트워크 보안 요건을 지원합니다. Always-On 지능형 VPN 은 AnyConnect 클라이언트 디바이스가 최적의 네트워크 액세스 포인트를 자동으로 선택하고 가장 효율적인 방법으로 터널링 프로토콜을 조정하도록 돕습니다. 여기에는 대기 시간에 민감한 트래픽을 위한 DTLS(Datagram Transport Layer Security) 프로토콜 및 Zero Trust 네트워크 액세스를 위한 경로가 포함됩니다. IPsec IKEv2(IP Security Internet Key Exchange version 2)에 대해서도 터널링 지원이 제공됩니다. 일부 애플리케이션 VPN 액세스는 Apple iOS 및 Google Android 에서 실행될 수 있습니다.

관리 VPN 터널은 최종 사용자가 VPN 연결을 설정하는 경우가 아니라 클라이언트 시스템의 전원이 켜 있을 때마다 기업 네트워크에 연결합니다. 결과적으로 사무실 외부 엔드포인트에서 패치 관리를 실행할 수 있는데, 특히 사용자가 VPN 을 통해 사무실 네트워크에 가끔 연결하는 디바이스에서 이 작업을 실행할 수 있습니다. 기업 네트워크 연결을 필요로 하는 엔드포인트 OS 로그인 스크립트도 이 기능의 도움을 받습니다. 이 기능에는 최종 사용자 인터페이스가 없습니다.

### Cisco Secure Endpoint

Windows 용 Cisco Secure Client 에서 사용 가능한 Secure Endpoint(보안 엔드포인트)는 Cisco Secure Client 내에서 모듈로 작동하며, Cisco Secure Client 사용자 인터페이스를 통해 액세스할 수 있습니다. Cisco Secure Endpoint Cloud 는 SecureX Cloud Management 와 마찬가지로 Cisco Secure Endpoint 와 함께 Cisco Secure Client 를 구축해도 됩니다. 고객은 이 통합을 활용하여 관리 중인 클라이언트 수를 줄일 수 있습니다.

### **클라우드 관리 모듈**

Cisco Secure Client 용 SecureX 클라우드 관리 구축을 사용하면, 관리자가 Cisco Secure Client 의 클라우드 관리 구축을 생성할 수 있습니다. 구축 구성은 엔드포인트에서 지정된 Cisco Secure Client 모듈의 클라우드에 연결하는 데 필요한 정보를 포함하는 경량 부트스트래퍼를 다운로드하는 옵션을 생성하고 관련 프로파일과 함께 구축합니다. 전체 설치 프로그램도 사용할 수 있습니다. 두 경우 모두 관리자는 기본 설정 소프트웨어 방법을 사용하여 엔드포인트에 설치 프로그램을 배포할 수 있습니다.

### Network Visibility Module

네트워크 가시성 모듈은 조직이 네트워크에서 엔드포인트 및 사용자 행동을 볼 수 있도록 고가치 엔드포인트 텔레메트리의 지속적인 피드를 제공합니다. 이는 온프레미스 및 오프프레미스 엔드포인트 및 사용자, 애플리케이션, 디바이스, 위치 및 대상과 같은 중요한 컨텍스트에서 플로우를 수집합니다. 이 데이터가 신뢰할 수 있는 네트워크(온프레미스 기업 네트워크 또는 VPN 을 통해)에 있을 때 이 데이터를 캐시하고 Network Visibility Module Collector 로 전송합니다. Network Visibility Module Collector(네트워크 가시성 모듈 컬렉터)는 IPFIX(Internet Protocol Flow Information Export) 데이터 및 Cisco Secure Network Analytics 엔드포인트 라이선스, 시스템 로그 또는 서드파티 컬렉터로 내보내는 선택적 필터를 수신하는 서버입니다. 네트워크 가시성 모듈 컬렉터는 nvzFlow 프로토콜 사양을 준수하는 수신 메시지를 처리합니다.

NVM 은 신뢰할 수 있는 네트워크에 있을 때만 플로우 정보를 전송합니다. 기본적으로는 데이터가 수집되지 않습니다. 데이터는 프로파일에 수집하도록 구성되어 있을 때만 수집되며 엔드포인트가 연결되어 있으면 계속 수집됩니다.

신뢰할 수 없는 네트워크에서 수집이 수행되는 경우에는 엔드포인트가 신뢰할 수 있는 네트워크에 있을 때 데이터가 캐시되어 전송됩니다. UI 없음

## Umbrella 로밍 보안 모듈

Umbrella 로밍 보안 서비스를 활용하려면 Professional, Insights, Platform 또는 MSP 패키지 구독이 필요합니다. Umbrella 로밍 보안은 활성 VPN 이 없을 때 DNS 레이어 보안을 제공하고 인텔리전트 프록시를 추가합니다. 또한 Cisco Umbrella 구독에서는 콘텐츠 필터링, 다양한 정책, 강력한 보고 기능, 기능적 디렉토리 통합 등도 제공합니다. 구독에 관계없이 동일한 Umbrella 로밍 보안 모듈을 사용합니다.

## ISE Posture 모듈

ISE Posture 는 Cisco Secure Client 제품의 추가 보안 구성 요소로 설치하도록 선택할 수 있는 모듈입니다. 모든 필수 요건을 충족하지 못하고 비준수로 간주되는 엔트포인트에 대해 엔드포인트 포스처 평가를 실행합니다. 다른 엔드포인트 승인 상태는 알 수 없는 포스처 또는 필수 요건 충족에 따른 규정 준수 상태입니다. 클라이언트는 헤드엔드에서 포스처 요건 정책을 수신하고, 포스처 데이터를 수집하며, 정책과 결과를 비교하여 헤드엔드에 평가 결과를 전송합니다. ISE 에서 엔드포인트의 규정 준수 여부를 결정하는 경우에도 Cisco Secure Endpoint 의 정책 평가를 사용합니다.

## Network Access Manager

Network Access Manager 는 사용자와 디바이스 ID 및 보안 액세스에 필요한 네트워크 액세스 프로토콜을 관리합니다. 또한 최종 사용자가, 관리자가 정의한 정책을 위반하는 연결을 하지 않도록 지능적으로 작동합니다. 이 소프트웨어는 정책에 따라 최적의 계층 2 액세스 네트워크를 탐지 및 선택하고 유선 및 무선 네트워크 액세스를 위한 디바이스 인증을 실행합니다.

## 포스처(Cisco Secure Firewall 용)

Cisco Secure Firewall 포스처는 Cisco Secure Firewall 이 엔드포인트 특성(운영 체제, IP 주소, 레지스트리 항목, 로컬 인증서, 파일 이름 등) 목록만 요청하는 경우 서버 측 평가를 실시하고, 이 특성들은 Cisco Secure Firewall 에서 반환됩니다. 정책의 평가 결과를 바탕으로 어떤 호스트가 보안 어플라이언스에 대해 원격 액세스 연결을 생성하도록 허용되는지 제어할 수 있습니다.

| 기능 | 장점 및 설명 |
|---|---|
| **원격 액세스** VPN/ZTNA | |
| **폭넓은 운영 체제 지원** | Windows 11(64 비트), 현재 Microsoft 지원 버전의 Windows 10 x86(32 비트) 및 x64(64 비트), Windows 8<br><br>ARM64 기반 Windows 11 의 Microsoft 지원 버전<br>ARM64 기반 Pc 용 Microsoft 지원 버전의 Windows 10<br>**참고**: Cisco Secure Client 5.0 **은** Windows 10/11 **전용입니다**. AnyConnect 는 위의 모든 것을 지원합니다.<br>macOS 12, 11.2, 10.15 및 10.14(모두 64 비트)<br>Red Hat<br>Ubuntu<br>SUSE(SLES)<br>모바일 데이터 시트에서 모바일 OS 지원에 대한 내용 참조 |

| 기능 | 장점 및 설명 |
| --- | --- |
| **소프트웨어 액세스** | Cisco.com Software Center 에서 다운로드가 가능합니다.<br>AnyConnect 에 대한 기술 지원 및 소프트웨어 이용 자격은 모든 기간 기반 Plus 및 Apex 라이센스에 포함되어 있으며, Plus 영구 라이센스용으로 별도로 구매 가능<br>계약 번호는 Cisco.com ID 와 연결되어야 합니다. Cisco Secure Client 주문 가이드에서 자세한 내용을 살펴보십시오. |
| **최적화된 네트워크 액세스**: VPN protocol choice SSL<br>(TLS **및** DTLS), IPsec IKEv2 | AnyConnect 에서는 VPN 프로토콜을 선택할 수 있으므로, 관리자가 비즈니스 요구에 가장 적합한 프로토콜 사용 가능<br>터널링 지원에는 SSL(TLS 1.2 및 DTLS 1.2) 및 차세대 IPsec IKEv2 포함<br>DTLS 는 VoIP 트래픽 또는 TCP 기반 애플리케이션 액세스 등 레이턴시에 민감한 트래픽에 맞게 최적화된 연결 제공<br>TLS 1.2(HTTP over TLS 또는 SSL)는 웹 프록시 서버를 사용하는 환경 등 제한된 환경에서 네트워크 연결의 가용성 보장<br>IPsec IKEv2 는 보안 정책에서 IPsec 을 사용해야 하는 경우 레이턴시에 민감한 트래픽에 맞게 최적화된 연결 제공 |
| **최적의 게이트웨이 선별** | 네트워크 액세스 포인트에 대해 최적화된 연결을 선택하므로, 최종 사용자는 가장 가까운 위치를 결정할 필요가 없음 |
| **모빌리티 지원** | 모바일 사용자를 위한 설계<br>IP 주소 변경, 연결 손실, 절전 또는 대기 모드 중에도 VPN 연결이 유지되도록 구성할 수 있음<br>Trusted Network Detection 기능을 통해 최종 사용자가 사무실에 있으면 자동으로 연결이 끊어지고, 원격 위치에 있으면 자동으로 연결되도록 VPN 연결 설정 가능 |
| **암호화** | TLS/DTLS 1.2 강력한 암호 지원<br>NSA Suite B 알고리즘, ESPv3 with IKEv2, 4096 비트 RSA 키, Diffie-Hellman 그룹 24, 확장 SHA2(SHA-256 & SHA-384)와 같은 차세대 암호화 IPsec IKEv2 연결에만 적용됨. Premier(이전 AnyConnect Apex)가 필요합니다. |
| **광범위한 배포 옵션** | **구축 옵션**:<br>사전 구축 - 엔터프라이즈 SMS(소프트웨어 관리 시스템)를 사용하거나 최종 사용자가 신규 설치 및 업그레이드를 실행합니다.<br>웹 구축 - Secure Firewall ASA, Secure Firewall Threat Defense 또는 ISE 서버인 헤드엔드에 Cisco Secure Client 패키지가 로드됩니다. 사용자가 방화벽이나 ISE 에 연결할 때, 클라이언트에 Cisco Secure Client 가 구축됩니다.<br>SecureX 클라우드 관리 구축 - Cisco Secure Client 5.0 은 맞춤형 구축을 사용하여 클라우드에서 구축할 수 있습니다. |

| 기능 | 장점 및 설명 |
| --- | --- |
| **다양한 인증 옵션** | **프로토콜**:<br>임베디드 또는 기본 브라우저(SSO)를 사용하는 SAML 2.0<br>RADIUS<br>LDAP<br>인증서.<br>TACACS+<br>HTTP 양식<br>SDI<br>Kerberos<br>**헤드엔드 방법**<br>AAA<br>AAA 및 인증서<br>인증서 전용<br>SAML<br>다중 인증서 및 AAA |
| **일관된 사용자 경험** | 전체 터널 클라이언트 모드는 LAN 과 같은 일관된 사용자 환경이 필요한 원격 액세스 사용자 지원<br>다중 전달 방법으로 AnyConnect 의 폭넓은 호환성 보장<br>관리자가 구성한 경우, 사용자가 클라이언트 소프트웨어의 업데이트 연기 가능<br>고객 경험 피드백 옵션 제공 |
| **중앙 집중식 정책 제어 및 관리** | 정책을 로컬에서 구성하거나 미리 구성할 수 있으며, VPN 보안 게이트웨이에서 자동으로 업데이트할 수 있음<br>웹 페이지 또는 애플리케이션을 통한 손쉬운 구축을 지원하는 AnyConnect 용 API<br>신뢰할 수 없는 인증서를 확인하여 사용자에게 경고<br>Cisco Secure Client 는 SecureX 플랫폼을 사용하여 구축 및 관리 지원 |
| **고급** IP **네트워크 연결** | IPv4 및 IPv6 네트워크와의 공개 연결<br>내부 IPv4 및 IPv6 네트워크 리소스에 액세스<br>관리자가 제어하는 스플릿 터널링(네트워크 및 동적 도메인) 및 전체 터널링 네트워크 액세스 정책<br>동적 액세스 정책 또는 ID 서비스 엔진을 사용하는 액세스 제어 정책<br>Apple iOS 및 Google Android 에 대한 앱별 VPN 정책<br>IP **주소 할당 메커니즘**:<br>고정<br>내부 풀<br>DHCP(Dynamic Host Configuration Protocol)<br>RADIUS/LDAP(Lightweight Directory Access Protocol) |

| 기능 | 장점 및 설명 |
| --- | --- |
| **강력한 통합 엔드포인트 규정 준수**<br>(**이전의** Apex **인** Premier **라이선스 필요**) | 유/무선 환경의 엔드포인트 보안 상태 평가 및 치료(Cisco Identity Services Engine NAC Agent 대체). Identity Services Engine(ISE) 1.3 이상과 Identity Services Engine Apex 라이선스 필요<br>ISE Posture(ISE 와 함께 연동) 및 Host Scan(VPN 전용)은 네트워크 액세스를 허용하기 전 엔드포인트 시스템에 악성코드 차단 소프트웨어, Windows 서비스 팩/패치 상태, 다양한 기타 소프트웨어 서비스가 있는지 여부를 확인함<br>관리자는 실행 중인 프로세스의 존재 여부를 기반으로 사용자 지정 상태 확인을 정의할 수 있습니다.<br>ISE Posture 및 Host Scan 은 원격 시스템에서 워터마크 존재 유무를 탐지할 수 있습니다. 워터마크는 기업 소유의 자산을 식별하는 데 사용할 수 있으며 그에 따라 차별화된 액세스를 제공함. 워터마크 확인 기능에는 시스템 레지스트리 값, 필요한 CRC32 체크섬과 일치하는 파일 존재 유무, 다양한 기타 기능이 포함됨. 규정 위반 애플리케이션에 대한 추가 기능 지원 |
| **클라이언트 방화벽 정책** | 스플릿 터널링 컨피그레이션을 위한 추가적인 보호 기능 제공<br>AnyConnect 및  Cisco Secure Client 와 함께 사용할 경우 로컬 액세스 예외 허용 가능(예: 인쇄, 테더링 디바이스 지원 등)<br>IPv4 용 포트 기반 규칙 및 IPv6 용 네트워크/IP ACL(Access Control List) 지원<br>Windows 및 Mac OS X 플랫폼에 사용 가능 |
| **현지화** | **영어 외에도 다음 언어가 지원됩니다**.<br>cs-CZ 체코어(체코)<br>de-DE 독일어(독일)<br>es-ES 스페인어(스페인)<br>fr-CA 프랑스어(캐나다)<br>fr-FR 프랑스어(프랑스)<br>hu-HU 헝가리어(헝가리)<br>it-IT 이탈리아어(이탈리아)<br>ja-JP 일본어(일본)<br>ko-KR 한국어(대한민국)<br>nl-NL 네덜란드어(네덜란드)<br>pl-PL 폴란드어(폴란드)<br>pt-BR 포르투갈어(브라질)<br>ru-RU 러시아어(러시아)<br>zh-CN 중국어(중국)<br>zh-HANS 중국어(간체)<br>zh-HANT 중국어(번체)<br>zh-TW 중국어(대만) |

| 기능 | 장점 및 설명 |
| --- | --- |
| **간편한 클라이언트 관리** | 관리자는 헤드엔드(Head-end) 보안 어플라이언스에서 소프트웨어 및 정책 업데이트의 자동 구축이 가능하므로, 클라이언트 소프트웨어 업데이트와 관련된 관리 작업이 없어집니다. 또한 Cisco Secure Client 5.0 은 관리자에게 SecureX Cloud 에서 클라이언트를 구축하고 관리할 수 있는 기능을 제공합니다.<br>관리자는 최종 사용자 구성을 위해 어떤 기능을 사용할지를 결정할 수 있습니다.<br>도메인 로그인 스크립트를 사용할 수 없을 경우 관리자는 연결 및 연결 해제 시 엔드포인트 스크립트를 트리거할 수 있습니다.<br>관리자는 최종 사용자에게 표시될 메시지를 완전히 사용자 지정 및 현지화할 수 있습니다. |
| **프로파일 편집기** | Cisco ASDM(Adaptive Security Device Manager)에서 직접 AnyConnect 정책을 사용자 지정할 수 있습니다.<br>독립형 프로파일 편집기<br>SecureX Cisco Secure Client 프로파일 페이지 |
| **진단** | 온-디바이스 통계 및 로깅 정보 사용 가능<br>디바이스에서 로그를 볼 수 있음<br>로그를 Cisco 또는 관리자에게 분석용으로 이메일을 통해 손쉽게 보낼 수 있음 |
| FIPS(Federal Information Processing Standard) | FIPS 140-2 Level 2 규격(플랫폼, 기능 및 버전 제한 적용) |
| **보안 모빌리티 및 네트워크 가시성** | |
| Cisco Umbrella Roaming(Cisco Umbrella Roaming **라이선스 필요**) | Umbrella 로밍 보안 모듈을 사용하려면 Professional, Insights, Platform 또는 MSP 패키지가 포함된 Umbrella 로밍 보안 서비스 구독이 필요합니다. Umbrella 로밍 보안은 활성 VPN 이 없을 때 DNS 레이어 보안을 제공하고, Cisco Umbrella 구독으로 인텔리전트 프록시를 추가합니다. 또한 Cisco Umbrella 서브스크립션에서는 콘텐츠 필터링, 다양한 정책, 강력한 보고 기능, Active Directory 통합 기능 등도 제공합니다. 서브스크립션에 관계없이 동일한 Umbrella 로밍 보안 모듈이 사용됩니다.<br>• VPN 이 꺼져 있는 경우 로밍 디바이스에 대해 보안 적용<br>• 로밍 디바이스에서 자동으로 악성코드, 피싱 및 C2 콜백 차단<br>• 디바이스 위치와 관계없이 간단한 보호 방법 제공<br>VPN 이 꺼져 있거나 스플릿 터널(터널 외 통신에 적용)을 사용하는 경우 DNS 기반 보안을 적용하기 위해 엔드포인트 리디렉션 활용 |
| Network Visibility Module(**이전의** Apex **인** Premier **라이선스 필요**) | 사용자, 엔드포인트, 애플리케이션, 위치 및 대상에 대한 풍부한 상황 정보로 엔드포인트 플로우 포착<br>온프레미스 및 오프프레미스에서 유연한 수집 설정<br>애플리케이션 사용을 모니터링하여 잠재적인 동작 이상 징후 식별<br>보다 많은 정보에 입각한 네트워크 설계 결정 지원<br>사용량 데이터는 Cisco 네트워크 애널리틱스와 같은 NetFlow 분석 툴과 공유 가능 |

| 기능 | 장점 및 설명 |
| --- | --- |
| Cisco Secure Endpoint(**이전의** Advanced Malware Protection for Endpoints)<br><br>(Cisco Secure Endpoint **라이선스 별도 구매**) | Cisco Secure Client 는 AnyConnect VPN/ZTNA 및 Cisco Secure Endpoint 기능을 모두 제공합니다.<br><br>원격 엔드포인트까지 엔드포인트 위협 서비스를 확장하여 엔드포인트 위협 보호 범위 확대<br><br>보다 사전 대응적인 보호 기능을 제공하여 원격 엔드포인트에서 공격이 신속하게 완화되도록 보장<br><br>macOS 엔드포인트는 독립형 보안 엔드포인트 클라이언트를 계속 사용할 수 있습니다. |
| **네트워크 액세스 관리자 및** 802.1X | |
| **미디어 지원** | • 이더넷(IEEE 802.3)<br>• Wi-Fi(IEEE 802.11) |
| **네트워크 인증** | • IEEE 802.1X-2001, 802.1X-2004 및 802.1X-2010<br>• 기업이 단일 802.1X 인증 프레임워크를 구축하여 유선 네트워크 및 무선 네트워크 모두에 액세스할 수 있도록 지원<br>• 보안 수준이 높은 액세스에 필요한 사용자 및 디바이스 ID 와 네트워크 액세스 프로토콜 관리<br>• Cisco 의 통합 유/무선 네트워크에 연결하는 사용자의 경험 최적화 |
| EAP(Extensible Authentication Protocol) **방식** | • EAP-TLS(Transport Layer Security)<br>• 다음 inner method 를 사용하는 EAP-PEAP(Protected Extensible Authentication Protocol):<br>• EAP-TLS<br>• EAP-MSCHAPv2<br>• EAP-GTC(Generic Token Card)<br>• 다음 inner method 를 사용하는 EAP-FAST(Flexible Authentication via Secure Tunneling):<br>• EAP-TLS<br>• EAP-MSCHAPv2<br>• EAP-GTC<br>• 다음 inner method 를 사용하는 EAP-TTLS(Tunneled TLS):<br>• PAP(Password Authentication Protocol)<br>• CHAP(Challenge Handshake Authentication Protocol)<br>• Microsoft CHAP(MSCHAP)<br>• MSCHAPv2<br>• EAP-MD5<br>• EAP-MSCHAPv2<br>• LEAP(Lightweight EAP), Wi-Fi 전용<br>• EAP-MD5(Message Digest 5), 관리자가 구성, 이더넷 전용<br>• EAP-MSCHAPv2, 관리자가 구성, 이더넷 전용<br>• EAP-GTC, 관리자가 구성, 이더넷 전용 |
| **무선 암호화 방식(해당** 802.11 NIC **지원 필요)** | • 개방성<br>• WEP(Wired Equivalent Privacy)<br>• Dynamic WEP<br>• WPA(Wi-Fi Protected Access) Enterprise<br>• WPA2 Enterprise<br>• WPA Personal(WPA-PSK)<br>• WPA2 Personal(WPA2-PSK) |

| 기능 | 장점 및 설명 |
| --- | --- |
| **무선 암호화 프로토콜** | AES(Advanced Encryption Standard) 알고리즘을 사용한 CCMP(Counter mode with Cipher Block Chaining Message Authentication Code Protocol) |
| **세션 재개** | EAP-TLS, EAP-FAST, EAP-PEAP 및 EAP-TTLS 를 사용한 RFC2716(EAP-TLS) 세션 재개<br>EAP-FAST 스테이트리스 세션 재개 |
| **이더넷 암호화** | 미디어 액세스 제어: IEEE 802.1AE(MACsec)<br>키 관리: MKA(MACsec Key Agreement)<br>유선 이더넷 네트워크의 보안 인프라를 정의하여 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증 제공<br>네트워크의 신뢰할 수 있는 구성 요소 간 통신 보호 |
| **한 번에 하나의 연결**<br>(Network Access Manager **가 설치된** Windows **에만 해당**) | 네트워크에 대해 하나의 연결만 허용하고 나머지는 연결 해제<br>어댑터 간 브리징 없음<br>우선순위에 따라 자동으로 이더넷 연결 |
| **복잡한 서버 검증** | "ends with" 및 "exact match" 규칙 지원<br>이름 공통성이 없는 서버에 대해 30 여 개 규칙 지원 |
| EAP-Chaining(EAP-FASTv2) | 기업 자산인지 아닌지에 따라 액세스 차별화<br>단일 EAP 트랜잭션에서 사용자 및 디바이스 검증 |
| ECE(Enterprise Connection Enforcement) | 사용자가 올바른 기업 네트워크에만 연결하도록 보장<br>사용자가 사무실에서 서드파티 액세스 포인트에 연결하여 인터넷을 검색하지 못하도록 방지<br>사용자가 게스트 네트워크에 대한 액세스를 설정하지 못하도록 방지<br>번거로운 차단 목록 제거 |
| Next-generation encryption (Suite B) | 최신 암호화 표준 지원:<br>Elliptic Curve Diffie-Hellman 키 교환<br>ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 |
| **크리덴셜 유형** | • 인터랙티브 사용자 비밀번호 또는 Windows 비밀번호<br>• RSA SecurID 토큰<br>• OTP(One-time password) 토큰<br>• 스마트 카드(Axalto, Gemplus, SafeNet iKey, Alladin)<br>• X.509 인증서<br>• ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서 |

## 플랫폼 호환성

Secure Client 는 다양한 Cisco Secure Firewall, Meraki 디바이스, Cisco Secure Connect Choice 및 Cisco Secure Connect Flex 와 호환됩니다. 가장 최근에 릴리즈된 소프트웨어를 이용하여 구축하는 것이 좋습니다.

추가 호환성 정보는 https://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html 에서 찾아볼 수 있습니다.

## 라이선스 옵션

Secure Client Advantage, Premium 또는 VPN 전용 라이선스가 필요합니다. 유효한 AnyConnect Plus, Apex 또는 VPN 전용 라이선스가 있는 고객은 Cisco Secure Client 를 활용할 수 있습니다.

라이선스 옵션과 주문에 대한 세부 내용을 주문 가이드 https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-client-og.html 에서 확인할 수 있습니다.

## Cisco Capital

**목표 달성에 도움이 되는 유연한 결제 솔루션**

Cisco Capital 을 사용하면 보다 쉽게 올바른 기술을 획득하여 목표를 달성하고 비즈니스를 혁신하며 경쟁력을 유지할 수 있습니다. 시스코에서는 고객이 총 소유 비용을 줄이고, 자본을 절약하며, 성장을 가속화하도록 지원합니다. 시스코의 유연한 결제 솔루션을 사용하면 100 개가 넘는 국가에서 하드웨어, 소프트웨어, 서비스 및 상호 보완적인 타사 장비를 쉽고 예측 가능한 결제 방식으로 구매할 수 있습니다. 자세히 알아보기.

## 자세히 알아보기

- Cisco Secure Client 홈페이지: https://www.cisco.com/go/secureclient
- Cisco Secure Client(이전의 AnyConnect) 설명서: https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
- 모바일 플랫폼용 Cisco Secure Client(이전의 AnyConnect) 데이터 시트: https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/data_sheet_c78-527494.html
- Cisco ASA 5500-X Series Adaptive Security Appliances: https://www.cisco.com/go/asa
- Cisco Secure Endpoint: https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoints/index.html
- Cisco Secure Client(이전의 AnyConnect)– 라이선스 계약 및 개인정보 보호정책: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html

**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,
The Netherlands

Cisco 는 전 세계에 200 개가 넘는 지사를 운영하고 있습니다. Cisco 웹사이트 https://www.cisco/go/offices 에서 주소, 전화번호 및 팩스 번호를 확인하십시오.



미국에서 인쇄 C78-3117430-00 07/22