

Cisco AnyConnect Secure Mobility Client for Mobile Platforms

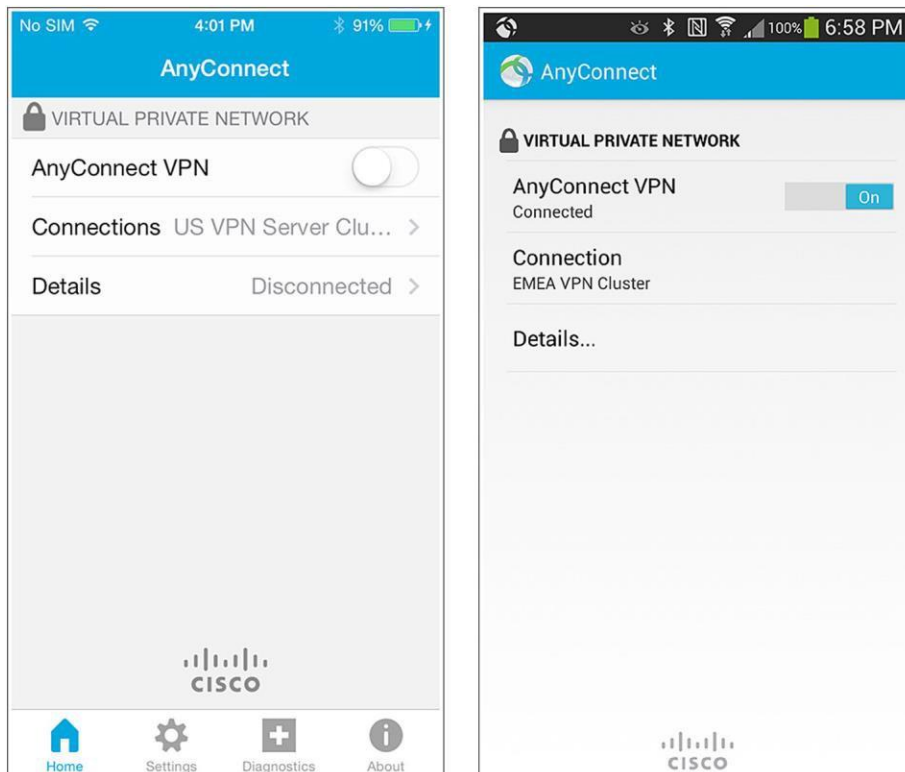
제품 개요

이제 Apple iOS 6.0+, Android 4.0+, 일부 Amazon Kindle 및 Fire Phone 장치에서 Cisco AnyConnect® Secure Mobility Client for Mobile Platforms로 직원의 스마트폰과 태블릿을 보호할 수 있습니다.

Cisco AnyConnect Secure Mobility Client for Mobile Platforms는 스마트폰과 태블릿을 위해 안정적이고 구축하기 편리한 암호화된 네트워크 연결을 제공하며, 이를 통해 이동 중인 직원이 지속적으로 기업 시스템에 액세스할 수 있습니다. Cisco AnyConnect 클라이언트는 업무용 이메일, 가상 데스크톱 세션, 기타 엔터프라이즈 애플리케이션에 액세스하는 어떤 경우에도 비즈니스 크리티컬 정보와 연결되는 편리한 인터페이스를 제공합니다. 이 클라이언트는 DTLS(Datagram Transport Layer Security), IPsec(IKEv2), TLS(HTTP over TLS/SSL)를 사용하여 기업 리소스에 대한 암호화된 액세스를 통해 비즈니스 크리티컬 애플리케이션을 제공합니다. 여기에는 VoIP(voice-over-IP)와 같이 대기 시간에 민감한 애플리케이션도 포함됩니다. Cisco AnyConnect 4.0은 iOS 7.0+에서 앱별 VPN 기능을 지원합니다.

그림 1은 Apple iOS와 Android 장치의 샘플 Cisco AnyConnect 사용자 인터페이스입니다.

그림 1. Apple iOS 및 Android 장치의 Cisco AnyConnect 사용자 인터페이스



기능 및 장점

표 1에서는 Cisco AnyConnect Secure Mobility Client for Mobile Platforms의 기능과 장점을 소개합니다.

표 1. 기능 및 장점

기능	혜택
소프트웨어 액세스 및 호환성	<p>애플리케이션 마켓플레이스에서 이용 가능</p> <ul style="list-style-type: none"> • Apple App Store: Apple iOS 6.0+ 장치 • Google Play: Android 4.0+ 장치 <p>여러 Cisco AnyConnect 이미지가 있으므로 장치에 적합한 이미지를 선택해야 합니다. 자세한 요구 사항은 Android 릴리스 정보를 참조하십시오.</p> <ul style="list-style-type: none"> • Amazon Appstore: 일부 Kindle 및 Fire Phone 장치에서 지원
최적화된 네트워크 액세스	<ul style="list-style-type: none"> • 네트워크 제약 조건에 따라 가장 효율적인 방식으로 터널링을 자동 조정합니다. • TCP 기반 애플리케이션 액세스 및 대기 시간에 민감한 트래픽(예: VoIP 트래픽)을 위해 최적화된 연결을 제공하는 데 DTLS를 사용합니다. • 잠긴 환경을 지나는 네트워크 연결의 가용성을 보장하기 위해 TLS(HTTP over TLS/SSL)를 사용합니다. • 보안 정책상 IPsec를 사용해야 하는 경우 IPsec/IKEv2에서 대기 시간에 민감한 트래픽을 위해 최적화된 연결을 제공합니다(ASA 8.4+ 필요). • Cisco ASA VPN 로드 밸런싱과의 호환성
모빌리티 지원	<ul style="list-style-type: none"> • IP 주소 변경, 연결 중단, 장치 대기 모드 이후 투명하게 재시작합니다. • 기업의 신뢰받는 네트워크에 연결된 경우 TND(Trusted Network Detection)에서 VPN 세션을 일시 중지하거나 연결을 끊습니다. <p>플랫폼 제한 때문에 일반 Android 또는 Apple iOS에서는 TND를 사용할 수 없습니다.</p>
배터리 절약	<ul style="list-style-type: none"> • Apple iOS 장치의 장치 슬립 작동과의 호환성
암호화	<ul style="list-style-type: none"> • AES-256, 3DES-168과 같은 강력한 암호화를 지원합니다. 보안 게이트웨이 장치에서 강력한 암호 라이선스가 설정되어 있어야 합니다. • NSA Suite B 알고리즘, ESPv3 with IKEv2, 4096비트 RSA 키, Diffie-Hellman 그룹 24, 확장 SHA2(SHA-256 & SHA-384)와 같은 차세대 암호화. IPsec IKEv2 연결에서만 사용 가능합니다. AnyConnect APEX 라이선스가 필요합니다.
인증 옵션	<ul style="list-style-type: none"> • RADIUS • NTLM(NT LAN Manager)에 대한 비밀번호 만료(MSCHAPv2)가 포함된 RADIUS • RADIUS OTP(1회 비밀번호) 지원(상태/응답 메시지 특성) • RSA SecurID • Active Directory/Kerberos • 디지털 인증서(인증서 배포 시 Cisco AnyConnect 통합 SCEP와의 호환성) • 일반 LDAP(Lightweight Directory Access Protocol) 지원 • 비밀번호 만료 또는 기한 경과가 포함된 LDAP • 인증서 및 사용자 이름/비밀번호 다중 팩터 인증 결합(이중 인증)
일관성 있는 사용자 환경	<ul style="list-style-type: none"> • 전체 터널 클라이언트 모드는 LAN과 같은 일관된 사용자 환경이 필요한 원격 액세스 사용자 지원
중앙 집중식 정책 제어 및 관리	<ul style="list-style-type: none"> • 정책을 로컬에서 구성하거나 미리 구성할 수 있으며, VPN 보안 게이트웨이에서 자동으로 업데이트할 수 있음 • Cisco AnyConnect를 위한 URI(Universal Resource Indicator) 핸들러로 웹 페이지 또는 애플리케이션에 내장된 URL을 통해 손쉽게 배포 • 인증서를 로컬에서 리포팅 관리할 수 있음
고급 IP 네트워크 연결	<ul style="list-style-type: none"> • 관리자가 제어하는 분할 또는 전체 터널링 네트워크 액세스 정책 • iOS 7+에서는 애플 VPN 정책(Cisco AnyConnect 4.0의 새로운 기능: Cisco ASA 5500-X, OS 9.3+ AnyConnect 4.0 라이선스 필요) • 액세스 제어 정책 <p>IP 주소 할당 메커니즘:</p> <ul style="list-style-type: none"> • 정적 • 내부 풀 • DHCP(Dynamic Host Configuration Protocol) • RADIUS/LDAP

기능	혜택
현지화	<p>영어 외에도 다음 언어가 지원됩니다.</p> <ul style="list-style-type: none"> • 캐나다 프랑스어 (fr-ca) • 체코어 (cs-cz) • 독일어 (de-de) • 일본어 (ja-jp) • 한국어 (ko-kr) • 라틴 아메리카 스페인어 (es-co) • 폴란드어 (pl-pl) • 중국어 간체 (zh-cn)
진단	<ul style="list-style-type: none"> • 장치에 대한 통계 및 로깅 정보 • 장치에 대한 로그 보기 • 로그를 Cisco 또는 관리자에게 분석용으로 이메일을 통해 손쉽게 보낼 수 있음

플랫폼 호환성

Cisco AnyConnect Secure Mobility Client는 ASA 소프트웨어 릴리스 8.0(4) 이상을 실행하는 모든 [Cisco ASA 5500-X Series Adaptive Security Appliance](#) 모델과 호환됩니다. 최신 ASA 소프트웨어 릴리스를 사용하는 것이 좋습니다.

특정 기능을 사용하려면 최신 Cisco ASA 소프트웨어 릴리스 또는 ASA 5500-X 모델이 필요합니다.

Cisco는 고급 보안 게이트웨이로 Cisco IOS® Release 15.1(2)T 이상의 기능에 대한 Cisco AnyConnect VPN 액세스를 지원합니다(일부 기능 제한). 자세한 내용은 [Cisco IOS SSL VPN에서 지원되지 않는 기능](#)을 참조하십시오.

추가적인 Cisco IOS 기능 지원 정보는 <http://www.cisco.com/go/fn>을 참조하십시오.

추가 호환성 정보는 다음에서 찾아볼 수 있습니다.

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html>.

Cisco AnyConnect Secure Mobility Client 라이선싱 옵션

라이선스 및 주문: Cisco AnyConnect 주문 가이드에서 AnyConnect 및 클라이언트리스 SSL VPN 사용 관련 라이선스 정책을 설명합니다.

<http://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/guide-c07-732790.html>

추가 Cisco ASA 5500-X 라이선싱 문서는 다음에서 찾아볼 수 있습니다.

<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html>.

추가 정보

- Cisco AnyConnect Secure Mobility Client 홈 페이지:
<http://www.cisco.com/go/anyconnect>
- Cisco AnyConnect 문서:
<http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html>
- Cisco ASA 5500-X Series Next-Generation Firewalls:
<http://www.cisco.com/go/asa>
- Cisco AnyConnect 라이선스 계약 및 개인정보 보호정책:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm

감사

본 제품에는 [OpenSSL 툴킷](#)에 사용하기 위한 목적으로 OpenSSL 프로젝트를 통해 개발된 소프트웨어가 포함되어 있습니다.

본 제품에는 [Eric Young](#)이 개발한 암호화 소프트웨어가 포함되어 있습니다.

본 제품에는 [Tim Hudson](#)이 개발한 소프트웨어가 포함되어 있습니다.

본 제품에는 libcurl HTTP 라이브러리가 통합되어 있습니다. Copyright[®] 1996-2006, [Daniel Stenberg](#).



미주 지역 본부
Cisco Systems, Inc.
San Jose CA

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. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 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)