Cisco AnyConnect Secure Mobility Client 릴리스 4.0.x용 Android 사용 설명서

Revised: February 6, 2015,

AnyConnect 사용 설명서

AnyConnect 설치 및 시작

AnyConnect 개요

Android용 Cisco AnyConnect Secure Mobility Client는 엔터프라이즈 네트워크에 원활하고 안정적인 원격 액세스를 제공합니다. AnyConnect를 사용하면 설치된 애플리케이션이 엔터프라이즈 네트워크에 직접 연결된 것처럼 통신할 수 있습니다. 또한 AnyConnect는 환경 설정을 설정하고 AnyConnect의 모양과 작업을 제어하며 관리자가 권장하는 대로 장치에서 진단 도구와 기능을 사용할 수 있는 정교한 네트워킹 애플리케이션입니다.

AnyConnect는 모바일 장치 관리 소프트웨어와 함께 기업에서 사용할 수 있습니다. 이 경우 승인된 애플리케이션 집합에 대한 VPN 액세스를 장치 관리 규칙이 제한할 수 있으므로 이 규칙을 준수할 수 있도록 관리자와 협력하십시오. 귀하의 조직에서 Android용 AnyConnect 사용에 관한 추가 설명서를 제공할 수도 있습니다.

초기 설치 및 모든 업그레이드를 위한 애플리케이션은 Android 앱 스토어에서 제공됩니다. Cisco Adaptive Security Appliance(ASA)는 VPN에 대한 액세스를 허용하는 보안 게이트웨이입니다. 그러나 모바일 장치용 AnyConnect의 업데이트는 지원하지 않습니다.

개방형 소프트웨어 라이센스 알림

- 본 제품에는 OpenSSL 툴킷에 사용할 수 있도록 OpenSSL Project(http://www.openssl.org/)에서 개발한 소프트웨어가 포함되어 있습니다.
- 본 제품에는 Eric Young(eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다.
- 본 제품에는 Tim Hudson(tjh@cryptsoft.com)이 작성한 소프트웨어가 포함되어 있습니다.

지원되는 Android 장치

Samsung 장치

AnyConnect는 다음과 같은 Samsung 장치를 지원합니다.

- Samsung Knox 1.0을 실행하는 Samsung 장치

  이 장치의 사용자는 Samsung Knox AnyConnect 패키지를 설치해야 합니다.
- Android 5.0(Lollipop) 이상을 실행하는 장치

  이 장치의 사용자는 AnyConnect ICS+ 패키지를 설치해야 합니다.
- Android 4.0, 4.1 또는 4.4(Ice Cream Sandwich, Jelly Bean 또는 KitKat)를 실행하는 Samsung 장치

  사용자는 AnyConnect ICS+ 패키지 또는 기존 Samsung AnyConnect 패키지를 설치할 수 있습니다.

참고 기존 Samsung AnyConnect 패키지는 4.0 버전이 아직 출시되지 않았습니다. 이 패키지의 경우 AnyConnect 3.0 제품 정보를 참조하십시오.

- Android 4.0 이전 버전을 실행하는 Samsung 장치

  사용자는 기존 Samsung AnyConnect 패키지를 설치해야 합니다.

참고 이 패키지는 2011년 9월 이후에 생산되거나 업그레이드된 장치에 적용됩니다. 설치를 시도했으나 다음 오류 메시지 중 하나가 표시되는 경우 장치를 업그레이드하고 AnyConnect를 설치해야 합니다.

- "설치 오류: 알 수 없는 이유 -8"
- "같은 공유 사용자 ID를 사용하는 다른 애플리케이션과 호환되지 않습니다."

Kindle 장치

Cisco AnyConnect(Kindle 태블릿 에디션)는 Kindle Fire HD 장치 및 New Kindle Fire용으로 Amazon에서 이용할 수 있습니다. Kindle용 Anyconnect는 Android VPN Framework를 통해 지원되며 AnyConnect ICS+ 패키지와 기능이 동일합니다.

Android VPN Framework 장치

AnyConnect ICS+는 Android 4.0(Ice Cream Sandwich) 이상에서 AVF(Android VPN Framework)가 지원하는 VPN 연결을 제공합니다.

AVF는 기본 VPN 연결만 제공합니다. 이 기본 VPN 기능을 사용하는 AnyConnect 클라이언트는 브랜드별 패키지에서 사용할 수 있는 전체 VPN 기능 집합을 제공할 수 없습니다.

참고 Cisco는 Android 4.0 이상을 실행하는 지원되지 않는 장치의 경우 AVF AnyConnect 클라이언트를 권장합니다. 지원되는 장치는 Android 운영 체제의 버전과 관계없이 브랜드별 AnyConnect 클라이언트를 사용해야 합니다.

Android AnyConnect 애플리케이션 설치

참고 Android용 AnyConnect는 Android 마켓에서만 다운로드할 수 있습니다. Cisco 웹사이트에서 다운로드하거나 이후 보안 게이트웨이에 연결된 후 다운로드할 수 없습니다.

절차

단계 **1** 장치가 지원되는 장치인지 확인하고 적합한 브랜드별 AnyConnect 패키지를 설치하십시오.

Cisco에서 제공하는 브랜드별 AnyConnect 패키지는 이러한 장치에 필요한 모든 기능을 갖춘 VPN 연결을 제공합니다. 이러한 브랜드별 AnyConnect 클라이언트는 장치 공급업체와 협력하여 제공되며 지원되는 장치의 기본 AnyConnect 클라이언트입니다.

a) Samsung 장치의 경우 다음 지침에 따라 설치하십시오.

- Samsung Knox 1.0을 실행하는 Samsung 장치

  이 장치의 사용자는 Samsung Knox AnyConnect 패키지를 설치해야 합니다.

- Android 5.0(Lollipop) 이상을 실행하는 장치

  이 장치의 사용자는 AnyConnect ICS+ 패키지를 설치해야 합니다.

- Android 4.0, 4.1 또는 4.4(Ice Cream Sandwich, Jelly Bean 또는 KitKat)를 실행하는 Samsung 장치

  사용자는 AnyConnect ICS+ 패키지 또는 기존 Samsung AnyConnect 패키지를 설치할 수 있습니다.

  참고 기존 Samsung AnyConnect 패키지는 4.0 버전이 아직 출시되지 않았습니다. 이 패키지의 경우 AnyConnect 3.0 제품 정보를 참조하십시오.

- Android 4.0 이전 버전을 실행하는 Samsung 장치

  사용자는 기존 Samsung AnyConnect 패키지를 설치해야 합니다.

  참고 이 패키지는 2011년 9월 이후에 생산되거나 업그레이드된 장치에 적용됩니다. 설치를 시도했으나 다음 오류 메시지 중 하나가 표시되는 경우 장치를 업그레이드하고 AnyConnect를 설치해야 합니다.

  - "설치 오류: 알 수 없는 이유 -8"
  - "같은 공유 사용자 ID를 사용하는 다른 애플리케이션과 호환되지 않습니다."

b) Kindle 장치의 경우 Cisco AnyConnect(Kindle 태블릿 에디션)를 설치하십시오.

단계 **2** 장치가 Android 4.0(Ice Cream Sandwich) 이상을 실행 중인지 확인하고 AnyConnect ICS+를 설치하십시오.

이 AnyConnect 클라이언트는 Android 4.0(Ice Cream Sandwich) 이상에서 AVF(Android VPN Framework)가 지원하는 VPN 연결을 제공합니다. AVF는 기본 VPN 연결만 제공합니다. 이 기본 VPN 기능을 사용하는 AnyConnect AVF 클라이언트는 브랜드별 패키지에서 사용할 수 있는 전체 VPN 기능 집합을 제공할 수 없습니다.

AnyConnect 시작

절차

단계 **1** AnyConnect 앱을 시작하려면 AnyConnect 아이콘을 누르십시오.

단계 **2** 설치 또는 업그레이드 이후 AnyConnect를 처음 시작하는 경우 표시된 최종 사용자 라이센스 계약에 동의하고 계속 진행하십시오.

단계 **3** **Connection(**연결**)** > **Add New VPN Connection(**새 **VPN** 연결 추가**)**을 누르고 연결 항목을 구성하십시오. 자세한 내용은 연결 항목 수동으로 추가, 6 페이지를 참조하십시오.

단계 **4** (선택 사항) 현재 활성 VPN 연결에 관한 요약 및 자세한 통계를 보려면 **Details(**세부사항**)**를 누르십시오. AnyConnect 통계 보기를 참조하십시오.

단계 **5** (선택 사항) **Menu(**메뉴**)**를 누르고 다음을 선택하십시오.

- **Settings(**설정**)**: AnyConnect 애플리케이션 환경 설정을 지정합니다. 애플리케이션 환경 설정 지정을 참조하십시오.
- **Diagnostics(**진단**)**: 다음과 같은 진단 작업을 수행합니다.
  - 인증서 관리: Android 장치의 인증서 정보를 참조하십시오.
  - AnyConnect 프로파일 관리: AnyConnect 클라이언트 프로파일 정보를 참조하십시오.
  - AnyConnect 현지화 관리: 현지화 관리를 참조하십시오.
  - 로깅 및 시스템 정보 보기: 로그 메시지 보기를 참조하십시오.
- **About(**정보**)**: AnyConnect 버전 및 라이센스 정보를 봅니다. AnyConnect 버전 및 라이센스 표시를 참조하십시오.
- **Exit(**종료**):** AnyConnect를 종료합니다. AnyConnect 종료를 참조하십시오.

다음에 할 작업

관리자가 제공한 지침에 따라 네트워크에 대한 VPN 연결을 구성하고 설정하십시오.

VPN 연결 구성

VPN 연결을 설정하기 위해 AnyConnect에 필요한 사항은 다음과 같습니다.

- 네트워크 액세스를 위한 보안 게이트웨이 주소

  이 주소는 연결 항목에서 구성됩니다. 연결 항목은 AnyConnect 홈 화면에 나열됩니다. 활성 연결 항목은 AnyConnect 홈 화면 또는 연결 목록에서 식별됩니다. VPN 연결 항목은 장치에서 자동 또는 수동으로 구성됩니다.

- 성공적으로 연결을 완료한 인증 정보

이 정보는 기억해야 하는 사용자 이름 또는 비밀번호의 형식으로 되어 있거나 장치에 구성된 디지털 인증서에 포함됩니다. 일부 VPN 연결의 경우 두 인증 방법이 모두 필요할 수 있습니다. 디지털 인증서는 장치에서 자동 또는 수동으로 구성됩니다.

관리자의 지침에 따라 AnyConnect 클라이언트를 설정하십시오. 관리자는 연결 항목 및 디지털 인증서의 구성을 자동화하는 절차 또는 해당 엔터티를 수동으로 구성하는 적절한 정보를 제공합니다. 명확한 지침이 없는 경우 관리자에게 문의하십시오.

연결 항목 구성

연결 항목은 사설 네트워크에 액세스할 수 있는 보안 게이트웨이 및 다른 연결 특성을 지정합니다.

절차

연결 항목은 장치에서 다음과 같은 방법으로 자동 또는 수동으로 구성됩니다.

- 수동으로 구성됩니다.

  네트워크의 보안 게이트웨이 주소를 알고 있어야 합니다. 주소는 보안 게이트웨이의 도메인 이름 또는 IP 주소이며 사용자가 속한 그룹을 지정할 수 있습니다. 또한 다른 연결 특성을 지정할 수도 있습니다. 연결 항목 수동으로 추가 또는 수정을 참조하십시오.

- 엔터프라이즈 모바일 장치 관리 소프트웨어를 통해 구성됩니다. 장치 관리 프로파일은 장치의 General Settings(일반 설정)에서 확인할 수 있습니다.

- AnyConnect 연결 항목을 구성하기 위해 관리자가 제공한 링크를 클릭하면 자동으로 구성됩니다.

  해당 링크는 이메일에 포함되거나 웹 페이지에 게시될 수 있습니다. 이 기능을 장치에서 사용하려면 애플리케이션 환경 설정의 **External Control**(외부 제어)을 **Prompt**(매번 확인) 또는 **Enable**(활성화)로 설정해야 합니다. AnyConnect의 외부 사용 제어, 15 페이지를 참조하십시오.

- 연결 항목을 포함하는 AnyConnect 클라이언트 프로파일을 다운로드하는 보안 게이트웨이에 연결한 후 자동으로 구성됩니다. AnyConnect 클라이언트 프로파일 관리, 18 페이지를 참조하십시오.

연결 항목 수동으로 추가

VPN 연결 항목을 추가하여 연결하려는 VPN 보안 게이트웨이를 식별합니다.

절차

단계 **1** AnyConnect 홈 창에서 **Connection**(연결) > **Add New VPN Connection**(새 **VPN** 연결 추가)을 눌러 연결 편집기를 여십시오.
언제든지 연결 편집기에서 **Cancel**(취소)을 누를 수 있습니다.

단계 **2** (선택 사항) 연결 항목에 대한 설명이 포함된 이름을 입력하려면 **Description**(설명)을 선택하십시오.

해당 연결 항목의 고유한 이름을 입력하십시오. 지정하지 않는 경우 **Server Address(**서버 주소**)**가 기본값으로 사용됩니다. 키보드 디스플레이의 모든 문자, 공백, 숫자 또는 기호를 사용하십시오. 이 필드는 대/소문자를 구분합니다.

단계 **3** 보안 게이트웨이의 주소를 입력하려면 **Server Address(**서버 주소**)**를 선택하십시오.
관리자가 지정한 경우 그룹을 포함하여 보안 게이트웨이의 도메인 이름 또는 IP 주소를 입력하십시오.

단계 **4** (선택 사항) 고급 인증서 및 프로토콜 설정을 변경하려면 **Advanced Preferences(**고급 환경 설정**)**를 누르십시오.
언제든지 고급 연결 편집기에서 **Cancel(**취소**)**을 누를 수 있습니다.

단계 **5** (선택 사항) 사용자 인증서가 해당 연결에 사용되는 방법을 지정하려면 **Certificate(**인증서**)**를 누르십시오.

- 인증서가 해당 연결에 사용되지 않도록 지정하려면 **Disabled(**비활성화**)**를 누르십시오.
- 인증서를 보안 게이트웨이로 요청된 경우에만 연결 설정하는 데 사용되도록 지정하려면 **Automatic(**자동**)**을 누르십시오.
- 관리자가 사용하도록 지시한 인증서를 누르십시오.

VPN 세션 설정에 필요한 경우 관리자는 모바일 장치에 사용자 인증서를 설치하기 위한 지침을 제공합니다. 자세한 내용을 보려면 목록에서 인증서를 누르십시오.

단계 **6** (선택 사항) 해당 VPN 연결에 SSL 대신 IPsec을 사용하려면 **Connect with IPsec(IPsec**과 연결**)**을 누르십시오.
해당 연결 특성은 관리자가 제공합니다.

VPN 연결 프로토콜에 대해 IPsec을 선택하는 경우 **Authentication(**인증**)** 매개변수가 활성화됩니다.

단계 **7** (선택 사항) **Authentication(**인증**)**을 누르고 해당 IPsec 연결의 인증 방법을 선택하십시오.
해당 연결 특성은 관리자가 제공합니다.

- EAP-AnyConnect(기본 인증 옵션)
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

Advanced Connection Editor(고급 연결 편집기**)** 창에 인증 옵션이 표시됩니다.

단계 **8** (선택 사항) EAP-GTC, EAP-MD5 또는 EAP-MSCHAPv2가 인증에 사용되도록 지정한 경우 **IKE Identity(IKE ID)**를 눌러서 관리자가 제공한 ID 정보를 입력하십시오.

단계 **9** **Advanced(**고급**)** 창과 **Connection Editor(**연결 편집기**)** 창에서 모두 **Done(**완료**)**을 눌러서 연결 값을 저장하십시오.
AnyConnect에서 새 연결 항목을 추가합니다.

연결 항목 수정

구성 오류를 수정하고 IT 정책 변경 사항을 준수하기 위해 VPN 연결 항목을 변경하십시오.

참고 보안 게이트웨이에서 다운로드된 연결 항목의 설명이나 서버 주소는 수정할 수 없습니다.

절차

단계 **1** AnyConnect 홈 창에서 **Connection(**연결**)**을 누르십시오. 그런 다음 연결 항목을 길게 누르면 **Select Action(**작업 선택**)** 창이 표시됩니다.

단계 **2** **Edit connection(**연결 수정**)**을 누르십시오.
연결 항목으로 할당된 매개변수 값이 **Connection Editor(**연결 편집기**)** 창에 표시됩니다.

단계 **3** 수정할 값을 누른 다음 화면 키보드를 사용하여 새 값을 입력한 후 **OK(**확인**)**를 누르십시오.

단계 **4** **Done(**완료**)**을 누르십시오.
AnyConnect에서 수정된 연결 항목을 저장합니다.

연결 항목 삭제

이 절차는 수동으로 구성된 VPN 연결 항목을 삭제합니다. VPN 보안 게이트웨이에서 가져온 연결 항목을 제거하는 유일한 방법은 연결 항목을 포함하는 다운로드된 AnyConnect 프로파일을 제거하는 것입니다.

절차

단계 **1** AnyConnect 홈 창에서 **Connection(**연결**)**을 누르십시오. 그런 다음 연결 항목을 길게 누르면 **Select Action(**작업 선택**)** 창이 표시됩니다.

단계 **2** **Delete connection(**연결 삭제**)**을 누르십시오.

인증서 구성

Android 장치의 인증서 정보

인증서는 VPN 연결의 각 종단 즉, 보안 게이트웨이 또는 서버와 AnyConnect 클라이언트 또는 사용자를 디지털 방식으로 식별하는 데 사용됩니다. 서버 인증서는 AnyConnect에 대한 보안 게이트웨이를 식별하고 사용자 인증서는 보안 게이트웨이에 대한 AnyConnect 사용자를 식별합니다. 인증서는 CA(Certificate Authorities: 인증 기관)에서 발급하고 확인합니다.

연결을 설정할 때 AnyConnect는 항상 보안 게이트웨이의 서버 인증서를 요구합니다. 보안 게이트웨이는 AnyConnect의 인증서가 필요하도록 구성된 경우에만 AnyConnect의 인증서를 요구합니다. VPN 연결을 인증하는 또 다른 방법으로 AnyConnect

사용자에게 수동으로 자격 증명 입력을 요구합니다. 실제로 보안 게이트웨이는 디지털 인증서, 수동으로 입력한 자격 증명 또는 두 가지를 모두 사용하여 AnyConnect 사용자를 인증하도록 구성할 수 있습니다. 인증서만 사용하는 인증을 통해 VPN이 사용자 간섭 없이 연결될 수 있습니다.

보안 게이트웨이와 장치로의 배포 및 보안 게이트웨이와 장치에 의한 인증서 사용은 관리자가 지정합니다. 관리자가 제공한 지침에 따라 AnyConnect VPN에 대한 서버 및 사용자 인증서 가져오고 사용하며 관리하십시오. 본 설명서에서는 사용자의 이해와 참조를 위해 인증서 및 인증서 관리에 관련된 정보와 절차를 제공합니다.

AnyConnect는 Android 장치의 자체 인증서 저장소의 인증을 위해 사용자 및 서버 인증서를 모두 저장합니다. AnyConnect 인증서 저장소는 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Certificate Management(**인증서 관리**)** 화면에서 관리됩니다. 또한 Android 시스템 인증도 여기에서 볼 수 있습니다.

사용자 인증서 정보

AnyConnect 사용자가 디지털 인증서를 사용하여 보안 게이트웨이에 대해 인증하려면 장치의 AnyConnect 인증서 저장소에 사용자 인증서가 있어야 합니다. 관리자의 지시에 따라 다음 방법 중 하나를 사용하여 사용자 인증서를 가져옵니다.

- 이메일 또는 웹 페이지에서 관리자가 제공한 하이퍼링크를 클릭하여 자동으로 가져옵니다.
- 장치의 파일 시스템, 장비의 인증서 저장소 또는 네트워크 서버에서 수동으로 가져옵니다.
- 인증서를 제공하기 위해 관리자가 구성한 보안 게이트웨이에 연결할 때 가져옵니다.

인증서를 가져온 후에는 인증할 연결을 설정하는 동안 특정 연결 항목에 연결되거나 자동으로 선택될 수 있습니다.

더 이상 인증이 필요하지 않은 경우, AnyConnect 저장소에서 사용자 인증서를 삭제할 수 있습니다.

서버 인증서 정보

연결 설정 중에 보안 게이트웨이에서 수신한 서버 인증서는 AnyConnect에 대한 해당 서버가 유효하고 신뢰할 수 있는 경우에만 자동으로 인증합니다. 그렇지 않을 경우,

- 유효하지만 신뢰할 수 없는 서버 인증서는 검토하고 권한을 부여하며 AnyConnect 인증서 저장소로 가져올 수 있습니다. 서버 인증서를 AnyConnect 저장소로 가져오면 이러한 디지털 인증서를 사용하는 서버로 생성된 후속 연결이 자동으로 수락됩니다.
- 유효하지 않은 인증서는 AnyConnect 저장소로 가져올 수 없습니다. 현재 연결을 완료하기 위해 수락될 수 있으나 이러한 구성은 권장하지 않습니다.

AnyConnect 저장소의 서버 인증서는 인증을 위해 더 이상 필요하지 않을 경우 삭제할 수 있습니다.

하이퍼링크를 통해 인증서 가져오기

관리자가 장치에 인증서를 설치할 수 있는 하이퍼링크를 제공합니다.

시작하기 전에

AnyConnect 설정에서 **External Control(**외부 제어**)**을 **Prompt(**매번 확인**)** 또는 **Enable(**활성화**)**로 설정하십시오.

절차

단계 **1** 관리자가 제공한 하이퍼링크를 누르십시오.

링크는 이메일에 포함되거나 인트라넷 웹 페이지에 게시될 수 있습니다.

단계 **2** 메시지가 나타나면 제공된 인증서의 인증 코드를 입력하십시오.

인증서는 Android 장치의 AnyConnect 인증서 저장소에 설치되며 확인, 연결 항목으로 할당, 또는 제거할 수 있습니다.

인증서 수동으로 가져오기

다음에서는 VPN 인증을 위해 AnyConnect 저장소로 사용자 인증서를 수동으로 가져오는 모든 가능한 옵션을 설명합니다.

시작하기 전에

관리자로부터 특정 인증서 가져오기 절차를 알아 두십시오.

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Certificate Management(**인증서 관리**)**를 누르십시오.

단계 **2** **User(**사용자**)** 탭을 누르십시오.

단계 **3** 인증서를 가져오려면 **Import(**가져오기**)**를 누르십시오.

단계 **4** 다음과 같이 가져오기 소스를 선택하십시오.

- 로컬 파일 시스템에서 인증서 파일을 가져오려면 **File System(**파일 시스템**)**을 누르십시오.
- 네트워크의 서버에서 인증서를 가져오려면 **Network Location (URI)(**네트워크 위치**(URI))**을 누르십시오.
- 현재 장치 자격 증명 저장소에 있는 인증서에 연결하려면 **Device Credential Storage(**장치 자격 증명 저장소**)**를 누르십시오.

  소스 인증서가 AnyConnect 인증서 저장소에 실제로 복사되지 않습니다. 인증서가 자격 증명 저장소에서 제거된 경우 인증서의 링크도 제거됩니다.

  참고
  - 이 옵션은 Android 4.0(Ice Cream Sandwich) 이상 실행 장치에서만 사용할 수 있습니다.
  - Android 4.1(Jelly Bean)에서 장치 자격 증명 저장소의 인증서를 가져오려고 하면 클라이언트에서 "해당 Android 버전에서는 이 기능이 지원되지 않습니다."라는 오류 메시지를 표시합니다. Android 네이티브 저장소를 사용하는 대신 AnyConnect 저장소로 인증서를 바로 가져오십시오.

보안 게이트웨이가 제공하는 인증서 가져오기

시작하기 전에

관리자는 인증서 배포를 활성화하도록 보안 게이트웨이를 구성하고 해당 보안 게이트웨이에 대한 연결 정보를 제공합니다.

절차

단계 **1** AnyConnect를 여십시오.

단계 **2** **Choose a connection**(연결 선택) 영역에서 인증서를 모바일 장치에 다운로드할 수 있는 연결의 이름을 누르십시오.

단계 **3** 다운로드할 수 있는 연결이 있는 경우 **Get Certificate**(인증서 가져오기)를 누르거나 모바일 장치에 인증서를 다운로드하도록 구성된 그룹을 선택하십시오.

단계 **4** 관리자가 제공한 인증 정보를 입력하십시오.

보안 게이트웨이가 장치에 인증서를 다운로드합니다. VPN 세션의 연결이 끊어지고 인증서를 성공적으로 등록했다는 메시지를 받게 됩니다.

인증서 보기

AnyConnect 인증서 저장소로 가져온 사용자 및 서버 인증서와 Android 시스템 인증서를 볼 수 있습니다.

절차

단계 **1** AnyConnect 홈 창에서 **Menu**(메뉴) > **Diagnostics**(진단) > **Certificate Management**(인증서 관리)를 누르십시오.

단계 **2** AnyConnect 인증서 저장소의 인증서를 보려면 **User**(사용자) 또는 **Server**(서버) 탭을 누르십시오.

인증서를 길게 누르고 다음을 수행하십시오.

- 인증서의 내용을 보려면 **View certificate details**(인증서 세부사항 보기)를 누르십시오.
- AnyConnect 저장소에서 해당 인증서를 제거하려면 **Delete certificate**(인증서 삭제)를 누르십시오.

단계 **3** Android 자격 증명 저장소의 인증서를 보려면 **System**(시스템) 탭을 누르십시오.

인증서의 내용을 보려면 인증서를 길게 누른 후 **View certificate details**(인증서 세부사항 보기)를 누르십시오.

인증서 제거

AnyConnect 인증서 저장소의 인증서만 제거하십시오. 시스템 인증서 저장소의 인증서는 제거할 수 없습니다.

인증서는 개별적으로 삭제하거나 AnyConnect 인증서 저장소에서 한꺼번에 지울 수 있습니다.

단일 인증서 삭제

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Certificate Management(**인증서 관리**)**를 누르십시오.

단계 **2** AnyConnect 인증서 저장소에 사용자 또는 서버 인증서를 표시하려면 **User(**사용자**)** 또는 **Server(**서버**)** 탭을 누르십시오.

단계 **3** 인증서를 길게 누르십시오.

Certificate Options(인증서 옵션**)**가 표시됩니다.

단계 **4** **Delete certificate(**인증서 삭제**)**를 선택하고 해당 특정 인증서를 삭제할지 확인합니다.

모든 인증서 지우기

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Certificate Management(**인증서 관리**)**를 누르십시오.

단계 **2** AnyConnect 인증서 저장소에 사용자 또는 서버 인증서를 표시하려면 **User(**사용자**)** 또는 **Server(**서버**)** 탭을 누르십시오.

단계 **3** AnyConnect 인증서 저장소에서 모든 인증서를 제거하려면 **Clear All(**모두 지우기**)**을 누르십시오.

VPN 연결 설정

AnyConnect VPN 패널에 표시된 활성 연결과 관련된 확인란 또는 슬라이더를 누르거나 AnyConnect 홈 화면에 나열된 다른 연결 항목 중 하나를 선택하여 VPN에 연결합니다.

시작하기 전에

- 활성 Wi-Fi 연결 또는 VPN에 연결할 서비스 공급자에 대한 연결이 있어야 합니다.
- VPN 연결을 시작하려면 AnyConnect 홈 창의 **Choose a Connection(**연결 선택**)**에 최소 1개의 연결 항목이 있어야 합니다.
- VPN 연결을 완료하려면 보안 게이트웨이를 통해 예상한 인증 정보가 있어야 합니다.

절차

단계 **1** AnyConnect 홈 창으로 이동하십시오.

단계 **2** **Connection(**연결**)**을 누른 후 사용할 연결 항목을 누르십시오.

AnyConnect가 현재 사용 중인 모든 VPN 연결을 해제하고 VPN 연결을 초기화할 때 해당 연결 항목을 현재 연결로 설정합니다.

단계 **3** 필요한 경우 인증 프롬프트가 나타날 때 다음 중 하나를 수행하십시오.

- 사용자 이름과 비밀번호 자격 증명을 입력하십시오. 관리자가 이중 인증을 설정한 경우 2차 자격 증명을 요청하는 메시지가 표시될 수 있습니다.
- **Get Certificate(**인증서 가져오기**)**를 누르고 관리자가 제공한 인증서 등록 자격 증명을 입력하십시오. AnyConnect가 인증서를 저장하고 VPN 보안 게이트웨이에 다시 연결하여 인증을 위해 인증서를 사용합니다.

VPN 보안 게이트웨이 구성에 따라 AnyConnect가 AnyConnect 홈 창의 목록에 연결 항목을 추가할 수도 있습니다. AnyConnect 홈 창에서 첫 행은 VPN 연결이 설정되었음을 나타내는 확인 표시를 강조합니다.

참고 AnyConnect 홈 창에서 다른 VPN 연결을 누르면 현재 VPN 연결을 해제하고 누른 VPN 연결과 관련된 VPN 보안 게이트웨이를 연결합니다.

AnyConnect 알림에 응답

신뢰할 수 없는 VPN 서버 알림에 응답

표시된 신뢰할 수 없는 **VPN** 서버 알림 유형은 다음과 같이 신뢰할 수 없는 **VPN** 서버 차단 애플리케이션 환경 설정에 따라 다릅니다.

- 설정이 활성화되어 신뢰할 수 없는 **VPN** 서버**!** 차단 알림이 표시된 경우 다음을 선택할 수 있습니다.
  - 설정 및 차단 동작을 유지하려면 **Keep Me Safe(**사용자 보안 유지**)**를 선택하십시오.
  - 차단을 해제하려면 **Change Settings(**설정 변경**)**를 선택하십시오.

    Block Untrusted VPN Server(신뢰할 수 없는 **VPN** 서버 차단**)**를 변경한 후 VPN 연결을 다시 초기화하십시오.
- 설정이 비활성화되어 신뢰할 수 없는 **VPN** 서버**!** 차단 해제 알림이 표시된 경우 다음을 선택할 수 있습니다.
  - 신뢰할 수 없는 서버에 대한 VPN 연결을 중단하려면 **Cancel(**취소**)**을 선택하십시오.
  - 신뢰할 수 없는 서버에 연결하려면 **Continue(**계속**)**를 선택하십시오. 이 옵션은 권장하지 않습니다.
  - 인증서 세부사항을 보며 이후 승인을 위해 서버 인증서를 AnyConnect 인증서 보관소로 가져오고 계속 연결할지 결정하려면 **View Details(**세부사항 보기**)**를 선택하십시오.

다른 앱에 응답

장치를 보호하기 위해 AnyConnect는 외부 애플리케이션이 AnyConnect를 사용하려고 할 때 경고를 표시합니다. 이는 AnyConnect 애플리케이션 환경 설정 **External Control(**외부 제어**)**이 **Prompt(**매번 확인**)**로 설정된 경우에 발생합니다.

다음 프롬프트에 대한 응답으로 **Yes(**예**)**를 눌러도 되는지 관리자에게 문의하십시오.

- 다른 애플리케이션에서 AnyConnect가 호스트에 새 연결을 만들도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]
- 다른 애플리케이션에서 AnyConnect가 호스트에 연결되도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]
- 다른 애플리케이션에서 AnyConnect가 현재 연결을 해제하도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]
- 다른 애플리케이션에서 AnyConnect가 AnyConnect 인증서 저장소로 인증서 번들을 가져오도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]
- 다른 애플리케이션이 AnyConnect가 현지화 파일을 가져오도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]
- 다른 애플리케이션에서 AnyConnect가 프로파일을 가져오도록 요청했습니다. 이를 허용하시겠습니까? [예 | 아니요]

MMS 알림에 응답

AnyConnect VPN이 연결된 동안에는 멀티미디어(MMS) 메시지를 검색하거나 전송할 수 없습니다. MMS 검색 또는 전송을 시도하여 차단된 경우 상태 표시줄에 MMS 알림 아이콘이 표시됩니다. 이 알림을 승인하려면 다음을 수행하십시오.

절차

단계 **1** 알림을 보려면 알림 아이콘을 누르십시오.

단계 **2** 서비스 결과를 보려면 알림을 누르십시오.

단계 **3** 더 이상 MMS 알림을 수신하지 않으려면 **Do not show this again(**다시 표시 안 함**)** 확인란을 선택하십시오.

주의 해당 선택은 영구적입니다. 이후에 해당 작업을 이전 상태로 돌릴 수 없습니다.

단계 **4** **OK(**확인**)**를 누르십시오.

선택적 AnyConnect 구성 및 관리

AnyConnect 애플리케이션 설정 지정

장치 시동 시 AnyConnect 시작

장치에서 AnyConnect를 언제 시작할지 제어할 수 있습니다. 기본적으로 AnyConnect는 장치를 시동할 때 자동으로 시작되지 않습니다. 확인 표시를 한 경우, Launch at Startup(시동 시 시작)이 활성화됩니다.

참고 신뢰할 수 있는 네트워크 감지를 지정하는 프로파일을 다운로드하거나 가져온 경우, Launch at Startup(시동 시 시작)이 자동으로 활성화됩니다.

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Settings(**설정**)**를 누르십시오.

단계 **2** 해당 환경 설정을 활성화 또는 비활성화하려면 **Launch at Startup(**시동 시 시작**)** 확인란을 누르십시오.

AnyConnect 상태 표시줄 아이콘 숨기기

AnyConnect를 사용하지 않을 때 알림 표시줄의 AnyConnect 아이콘을 숨길 수 있습니다.

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Settings(**설정**)**를 누르십시오.

단계 **2** **Hide Icon(**아이콘 숨기기**)** 확인란을 누르십시오.

확인란의 확인 표시를 지우면 아이콘이 계속 표시됩니다.

AnyConnect의 외부 사용 제어

외부 제어 애플리케이션 설정에서 AnyConnect 애플리케이션이 외부 URI 요청에 응답하는 방법을 지정합니다. 외부 요청은 연결 항목을 생성하고 VPN을 연결하거나 연결 해제하며 클라이언트 프로파일, 인증서 또는 현지화 파일을 가져옵니다.

외부 요청은 일반적으로 관리자가 이메일 또는 웹 페이지에서 제공합니다. 관리자는 다음 값 중 하나를 사용하도록 지시합니다.

- Enabled(활성화) - AnyConnect 애플리케이션이 모든 URI 명령을 자동으로 허용합니다.
- Disabled(비활성화) - AnyConnect 애플리케이션이 모든 URI 명령을 자동으로 허용하지 않습니다.
- Prompt(매번 확인) - 장치에서 AnyConnect URI가 액세스될 때마다 AnyConnect 애플리케이션이 메시지를 표시합니다. URI 요청을 허용하거나 허용하지 않을 수 있습니다. 자세한 내용은 다른 앱에 응답, 14 페이지를 참조하십시오.

절차

단계 **1**	AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Settings(**설정**)**를 누르십시오.
단계 **2**	**External Control(**외부 제어**)**을 누르십시오.
단계 **3**	**Enabled(**활성화**)**, **Disabled(**비활성화**)** 또는 **Prompt(**매번 확인**)**를 누르십시오.

신뢰할 수 없는 서버 차단

이 애플리케이션 설정은 보안 게이트웨이를 식별할 수 없는 경우 AnyConnect의 연결 차단 여부를 결정합니다. 해당 보호 기능은 기본적으로 활성화되어 있고 비활성화할 수 있으나 권장하지 않습니다.

AnyConnect는 ID를 확인하기 위해 서버에서 수신한 인증서를 사용합니다. 만료되거나 유효하지 않은 날짜, 잘못된 키 사용 또는 이름 불일치로 인해 인증서 오류가 발생하는 경우 연결이 차단됩니다.

이 설정이 활성화된 경우 **Untrusted VPN Server!(**신뢰할 수 없는 **VPN** 서버**!)** 차단 알림에서 이러한 보안 위협을 알려줍니다.

절차

단계 **1**	AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Settings(**설정**)**를 누르십시오.
단계 **2**	해당 환경 설정을 활성화 또는 비활성화하려면 **Block Untrusted Servers(**신뢰할 수 없는 서버 차단**)** 확인란을 누르십시오.

FIPS 모드 설정

FIPS 모드는 모든 VPN 연결을 위해 FIPS(Federal Information Processing Standard:연방 정부 정보 처리 표준) 암호화 알고리즘을 사용합니다.

시작하기 전에

네트워크 연결을 위해 모바일 장치에 FIPS 모드를 활성화해야 하는 경우 관리자가 알려줍니다.

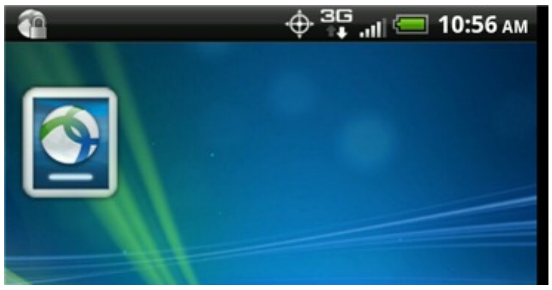
절차

단계 **1**	AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Settings(**설정**)**를 누르십시오.
단계 **2**	해당 환경 설정을 활성화 또는 비활성화하려면 **FIPS Mode(FIPS** 모드**)**를 누르십시오. FIPS 모드 전환이 확인되면 AnyConnect가 종료되므로 수동으로 다시 시작해야 합니다. 다시 시작할 때 FIPS 모드 설정이 적용됩니다.

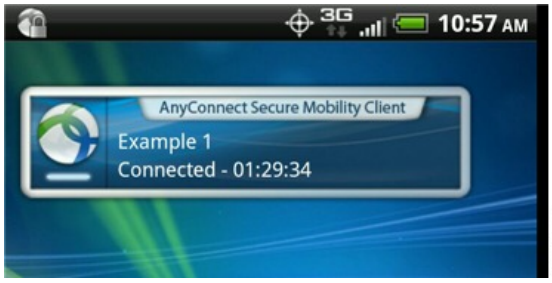
AnyConnect 위젯 사용

AnyConnect는 다음과 같이 홈 화면에 추가할 수 있는 위젯을 제공합니다.

- 가장 작은 위젯은 AnyConnect 앱 아이콘과 같은 크기입니다. 아이콘 아래에 있는 막대의 색은 VPN 상태를 나타냅니다. 현재 VPN 연결에서 연결 또는 연결 해제하려면 위젯을 누르십시오.



- 더 큰 위젯은 AnyConnect 아이콘과 이름, 현재 VPN 연결 및 VPN 상태를 표시합니다. 현재 VPN 연결에서 연결 또는 연결 해제하려면 위젯을 누르십시오.



위젯 배치에 관한 지침은 사용 중인 장치 및 Android 버전에 따라 다를 수 있습니다. 예제 지침이 제공됩니다.

절차

단계 **1**	사용하려는 위젯을 넣을 충분한 공간이 있는 Android 홈 화면으로 이동하십시오.
단계 **2**	**Menu**(메뉴) > **Personalize**(개인 설정) > **Widgets**(위젯)를 누르십시오.
단계 **3**	사용하려는 AnyConnect 위젯을 누르십시오. Android에서 홈 화면에 위젯을 추가합니다.
단계 **4**	위치를 변경하려는 경우 위젯을 길게 누릅니다. 응답하면 위젯을 옮기십시오.

AnyConnect 클라이언트 프로파일 관리

AnyConnect 클라이언트 프로파일 정보

AnyConnect VPN 클라이언트 프로파일은 클라이언트 동작을 지정하고 VPN 연결을 식별하는 XML 파일입니다. VPN 클라이언트 프로파일에 있는 각 연결 항목은 해당 장치에 액세스할 수 있는 보안 게이트웨이와 다른 연결 특성, 정책 및 제한을 지정합니다. 장치에서 로컬로 구성한 VPN 연결뿐만 아니라 이러한 연결 항목은 VPN 연결을 시작할 때부터 선택할 수 있도록 AnyConnect 홈 화면에 나열됩니다.

AnyConnect는 한 번에 하나의 VPN 클라이언트 프로파일만 Android 장치에 보관합니다. 다음은 존재할 경우 현재 프로파일을 교체하거나 삭제하는 일부 핵심 시나리오입니다.

- 프로파일을 수동으로 가져오면 현재 프로파일이 가져온 프로파일로 교체됩니다.
- 자동 또는 수동 VPN 연결 시작 시 새로운 연결의 프로파일이 현재 프로파일을 대체합니다.
- VPN 연결에 연결된 프로파일이 없는 경우 해당 VPN 시작 시 기존 프로파일이 삭제됩니다.

현재 장치의 AnyConnect 프로파일을 확인 또는 삭제하거나 새 프로파일을 가져오십시오.

AnyConnect 프로파일 보기

절차

단계 **1** AnyConnect 홈 창에서 **Menu**(메뉴) > **Diagnostics**(진단) > **Profile Management**(프로파일 관리)를 누르십시오.

단계 **2** **Current Profile Details**(현재 프로파일 세부사항)의 확장 아이콘을 누르십시오. XML 파일이 표시됩니다. 전체 파일을 보려면 스크롤을 내립니다.

AnyConnect 프로파일 가져오기

시작하기 전에

이 방법으로 프로파일 파일을 가져오려면 Android 장치에 프로파일 파일이 있어야 합니다. 관리자가 장치에 설치될 프로파일 파일의 이름을 제공합니다.

절차

단계 **1**	AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Profile Management(**프로파일 관리**)**를 누르십시오.
단계 **2**	**Import Profile(**프로파일 가져오기**)**을 누르고 장치의 파일 시스템에서 XML 프로파일을 선택합니다. 이 프로파일에 정의된 연결 항목은 AnyConnect 홈 화면에서 즉시 표시되며 AnyConnect 클라이언트 동작은 이 프로파일의 사양을 준수합니다.

AnyConnect 프로파일 제거

절차

단계 **1**	AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Profile Management(**프로파일 관리**)**를 누르십시오.
단계 **2**	**Delete Profile(**프로파일 삭제**)**을 누르고 현재 프로파일을 삭제할지 확인하십시오. 프로파일에 정의된 연결 항목이 AnyConnect 홈 화면에서 지워집니다. 또한 AnyConnect 클라이언트 동작은 기본 클라이언트 사양을 준수합니다.

현지화 관리

설치된 현지화 데이터 보기

AnyConnect를 설치할 때 장치의 지정 로캘이 패키지에 포함된 언어 번역 중 하나와 일치하는 경우 모바일 장치가 현지화됩니다. AnyConnect 패키지에는 다음 언어의 번역이 포함되어 있습니다.

- 체코어(cs-cz)
- 독일어(de-de)
- 라틴 아메리카 스페인어(es-co)
- 캐나다 프랑스어(fr-ca)
- 일본어(ja-jp)
- 한국어(ko-kr)
- 폴란드어(pl-pl)
- 중국어 간체(zh-cn)

설치된 언어는 **Settings(**설정**)** > **Language and Keyboard(**언어 및 키보드**)** > **Select locale(**로캘 선택**)**에서 지정한 로캘에 따라 결정됩니다. AnyConnect를 시작하는 즉시 AnyConnect UI 및 메시지가 번역됩니다.

AnyConnect는 일치도를 결정하기 위해 언어 사양을 사용한 다음 지역 사양을 사용합니다. 예를 들면 설치 후 프랑스어 - 스위스(fr-ch) 로캘을 설정하면 프랑스어 - 캐나다(fr-ca)가 표시됩니다.

절차

단계 **1** AnyConnect 홈 창에서 **Menu**(메뉴) > **Diagnostics**(진단) > **Localization Management**(현지화 관리)를 누르십시오.

단계 **2** 모바일 장치에 설치된 현지화 파일 목록을 확인하십시오.

지정된 언어는 현재 AnyConnect에서 사용하고 있는 언어입니다.

현지화 데이터 가져오기

설치 후 다음과 같은 방법으로 AnyConnect 패키지에서 지원하지 않는 언어의 현지화 데이터를 가져옵니다.

- 관리자가 제공한 하이퍼링크를 클릭합니다. 이 하이퍼링크는 현지화 데이터를 가져오도록 정의되어 있습니다.

  하이퍼링크는 관리자가 이메일 또는 웹 페이지에서 제공하며 클릭할 경우 현지화 데이터를 가져옵니다. 이 방법에서는 관리자가 AnyConnect 구성 및 관리를 단순화할 수 있는 기능인 AnyConnect URI 처리기를 사용합니다.

  참고 AnyConnect 설정에서 외부 제어를 Prompt(매번 확인) 또는 Enable(활성화)로 설정하여 AnyConnect 활동을 허용해야 합니다. 설정하는 방법은 AnyConnect의 외부 사용 제어, 15 페이지를 참조하십시오.

- VPN 연결을 통해 다운로드 가능한 현지화 데이터를 제공하기 위해 관리자가 구성한 보안 게이트웨이에 연결합니다.

  이 방법을 사용하는 경우 관리자가 XML 프로파일에서 적절한 VPN 연결 정보나 미리 정의된 연결 항목을 제공합니다. VPN 연결 시 현지화 데이터는 장치에 다운로드되고 즉시 적용됩니다.

- 아래에 설명된 대로 AnyConnect 현지화 관리 작업 화면의 **Import Localization**(현지화 가져오기) 옵션을 사용하여 수동으로 가져옵니다.

절차

단계 **1** AnyConnect 홈 창에서 **Menu**(메뉴) > **Diagnostics**(진단) > **Localization Management**(현지화 관리)를 누르십시오.

단계 **2** **Import Localization**(현지화 가져오기)을 누르십시오.

단계 **3** 보안 게이트웨이 및 로캘 주소를 지정하십시오.

로캘은 ISO 639-1에 따라 지정되며 필요한 경우 국가 코드가 추가됩니다(예 :en-US, fr-CA, ar-IQ 등).

해당 현지화 데이터는 이미 패키지에 포함되어 설치된 현지화 데이터 대신 사용됩니다.

현지화 데이터 복원

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Localization Management(**현지화 관리**)**를 누르십시오.

단계 **2** **Restore Localization(**현지화 복원**)**을 누르십시오.

AnyConnect 패키지에서 미리 로드한 현지화 데이터 사용을 복원하고 가져온 현지화 데이터를 모두 삭제합니다.

복원된 언어는 **Settings(**설정**)** > **Language and Keyboard(**언어 및 키보드**)** > **Select locale(**로캘 선택**)**에서 지정한 장치의 로캘에 따라 선택됩니다.

AnyConnect 종료

AnyConnect를 종료하여 현재 VPN 연결을 끝내고 모든 AnyConnect 프로세스를 중단합니다. 이 기능은 자주 사용하지 마십시오. 장치의 다른 앱 또는 프로세스가 현재 VPN 연결을 사용하고 있을 수 있으며 AnyConnect를 종료하면 해당 작동에 부정적인 영향을 줄 수 있습니다.

절차

AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Exit(**종료**)**를 누르십시오.

AnyConnect가 모든 프로세스를 정상적으로 종료할 수 없는 경우 **Force Stop(**강제 종료**)**을 누르면 Android 애플리케이션 관리 화면으로 우회하여 AnyConnect를 수동으로 종료할 수 있습니다.

AnyConnect 제거

절차

단계 **1** 장치의 Android 설정으로 이동하여 앱 또는 애플리케이션 관리 영역으로 이동합니다.

단계 **2** **Uninstall(**제거**)**을 누르십시오.

AnyConnect 모니터링 및 문제 해결

AnyConnect 버전 및 라이센스 표시

절차

AnyConnect 홈 창에서 **Menu(**메뉴**)** > **About(**정보**)**을 누르십시오.

다음에 할 작업

본 설명서의 최신 버전을 열려면 **About(**정보**)** 창에서 링크를 누르십시오.

AnyConnect 통계 보기

VPN이 연결되면 AnyConnect가 통계를 기록합니다.

절차

AnyConnect 홈 화면에서 **Details(**세부정보**)**를 누르십시오.

세부 통계는 다음 값을 포함합니다.

- 보안 경로 - 항목의 대상이 0.0.0.0이고 서브넷 마스크가 0.0.0.0이면 모든 VPN 트래픽이 암호화되고 VPN 연결을 통해 전송 또는 수신된 것을 의미합니다.
- 비보안 경로 - 보안 경로에 0.0.0.0/0.0.0.0이 나타날 때만 표시됩니다. 트래픽 대상은 VPN 보안 게이트웨이에서 결정한 대로 암호화된 연결에서 제외됩니다.

AnyConnect 로깅

로그 메시지 보기

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Logging and System Information(**로깅 및 시스템 정보**)**을 누르십시오.

AnyConnect가 메시지를 검색하고 Messages(메시지), System(시스템) 및 Debug(디버그) 창에 메시지를 표시합니다.

단계 **2** 로그 메시지 또는 시스템 정보를 보려면 **Messages(**메시지**)**, **System(**시스템**)** 또는 **Debug(**디버그**)** 탭을 누르십시오.

- Messages(메시지): AnyConnect 활동에 관련된 로그
- System(시스템): 메모리, 인터페이스, 경로, 필터, 권한, 프로세스, 시스템 속성, 메모리 맵 및 고유 장치 ID 관련 정보
- Debug(디버그): AnyConnect 문제를 분석하기 위해 관리자 및 Cisco Technical Assistance Center(TAC)에서 사용하는 로그

단계 **3** 모든 메시지를 보려면 창을 스크롤하십시오.

로그 메시지 전송

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Logging and System Information(**로깅 및 시스템 정보**)**을 누르십시오.

단계 **2** **Menu(**메뉴**)** > **Send Logs(**로그 전송**)**를 누르십시오.

로그 메시지 및 모든 프로파일 데이터는 .zip 파일로 패키지되어 이메일 메시지에 삽입됩니다. AnyConnect에 문제를 보고하는 경우 이메일 옵션을 사용하여 관리자에게 로그 파일을 전송하십시오. 로그 메시지를 전송하기 전에 문제를 재현하기 위해 문제 설명 및 단계를 지정해야 합니다.

로컬로 전송하려면 블루투스를 사용하십시오. 전송 장치와 수신 장치에서 블루투스를 먼저 활성화해야 합니다.

디버그 로그 메시지 지우기

절차

단계 **1** AnyConnect 홈 창에서 **Menu(**메뉴**)** > **Diagnostics(**진단**)** > **Logging and System Information(**로깅 및 시스템 정보**)**을 누르십시오.

단계 **2** **Menu(**메뉴**)** > **Clear Debug Logs(**디버그 로그 지우기**)**를 누르십시오.

일반적인 **Android** 문제

tun.ko 오류 메시지가 표시됨

tun.ko 모듈은 커널로 아직 컴파일되지 않은 경우에 필요합니다. tun.ko 모듈이 장치에 포함되거나 커널로 컴파일되지 않은 경우 해당하는 장치 커널에 대해 가져오거나 구축하고 /data/local/kernel_modules/ 디렉토리에 넣으십시오.

일부 연결 항목을 수정 또는 삭제할 수 없음

관리자가 AnyConnect 프로파일에서 해당 연결 항목을 정의했습니다. 해당 프로파일의 삭제 방법은 AnyConnect 프로파일 보기 및 관리를 참조하십시오.

연결 시간 초과 및 확인할 수 없는 호스트

인터넷 연결 문제, 낮은 셀 신호 수준 및 정체된 네트워크 리소스가 시간 제한 및 확인할 수 없는 호스트의 일반적인 원인입니다. 더욱 강한 신호가 있는 곳으로 이동하거나 WiFi를 사용하십시오. Wi-Fi 네트워크가 가까운 곳에 있는 경우, 장치 설정 앱을 사용하여 Wi-Fi 네트워크에 먼저 연결하도록 설정하십시오. 시간 초과 시 여러 번 다시 시도하면 성공할 수 있습니다.

인증서 기반 인증을 사용할 수 없음

이전에 사용한 경우 인증서의 유효성 및 만료를 확인하십시오. 이를 위해 AnyConnect 홈 창으로 이동하여 연결 항목을 길게 누른 후 **Certificate(**인증서**)**를 누르십시오. 인증서 창에 모든 인증서가 나열됩니다. 인증서 이름을 길게 누르고 **View Certificate Details(**인증서 세부사항 보기**)**를 누르십시오. 관리자에게 문의하여 연결에 적합한 인증서를 사용하고 있는지 확인하십시오.

연결 오류가 발생하지만 장치는 제대로 작동함

모바일 연결을 허용하도록 VPN 게이트웨이가 구성되고 라이센스를 받았는지 관리자에게 문의하십시오.

ASA에 연결할 수 없음**,** 확인할 수 없는 호스트 오류

인터넷 브라우저를 사용하여 네트워크 연결을 확인하십시오. 네트워크 연결성을 확인하려면 https://`vpn.example.com`으로 이동하십시오. 이때 `vpn.example.com`은 VPN 보안 게이트웨이의 URL입니다.

마켓에서 **AnyConnect** 패키지가 설치되지 않음

지원되는 Android 장치 목록에 해당 장치가 포함되어 있는지 확인하십시오.

"설치 오류**:** 알 수 없는 이유 **-8"**

지원되지 않는 장치에 브랜드별 AnyConnect 패키지를 설치하려는 경우 이 메시지를 받게 됩니다. 지원되는 Android 장치 목록 및 AnyConnect 설치 또는 업그레이드 지침을 검토하고 장치에 적절한 AnyConnect 패키지를 다운로드하십시오.

AnyConnect 오류**, "**이 애플리케이션의 실행에 필요한 권한을 얻지 못했습니다**."** 해당 장치가 **AnyConnect**를 지원하지 않습니다**.**

AnyConnect는 해당 장치에서 작동하지 않습니다. 지원되는 Android 장치 목록 및 AnyConnect 설치 또는 업그레이드 지침을 검토하고 장치에 적절한 AnyConnect 패키지를 다운로드하십시오.

네트워크 연결성 문제로 인해 로그를 이메일로 보낼 수 없음

인터넷 액세스가 가능한 다른 네트워크를 시도해보십시오. 네트워크가 연결되지 않았거나 장치를 리셋해야 할 경우, 로그 메시지를 임시 저장 이메일 메시지에 저장하십시오.

AnyConnect가 종종 저절로 연결됨

이는 TND(Trusted Network Detection: 신뢰할 수 있는 네트워크 감지) 또는 자동 VPN 정책이 원인일 수 있습니다. 이 기능을 해제하려면 AnyConnect 설정에서 TND 애플리케이션 환경 설정을 비활성화하십시오.

일회용 비밀번호를 사용하는 인증이 작동하지 않음

Android 문제로 인해 클립보드의 텍스트를 붙여 넣을 때 텍스트 앞에 공백이 삽입됩니다. AnyConnect에서 일회용 비밀번호와 같은 텍스트를 복사할 때 사용자는 이러한 잘못된 공백을 삭제해야 합니다.

Android용 AnyConnect의 알려진 문제

이 릴리스에는 다음과 같은 알려진 문제 및 버그가 있습니다.

- AnyConnect가 EDGE 연결을 통해 VPN 트래픽을 송신 또는 수신하는 경우, EDGE 및 기타 초기 무선 기술의 고유한 특성으로 인해 음성 통화가 차단됩니다.
- VPN이 연결되어 있는 동안 Android 보안 규칙으로 인해 MMS(multimedia messaging service: 멀티미디어 메시징 서비스) 메시지를 전송 및 수신할 수 없습니다. VPN이 연결되어 있는 동안 MMS 메시지 전송하려고 하면 대부분의 장치 및 서비스 공급자가 알림을 표시합니다. Android에서는 VPN이 연결되어 있지 않을 때 메시지 전송 및 수신을 허용합니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands