Cisco AnyConnect Secure Mobility Client, 릴리스 4.4 릴리스 노트

초판: 2016년 12월 13일

최종 변경: 2017년 05월 22일

AnyConnect Secure Mobility Client, 릴리스 4.4 릴리스 노트

이 릴리스 노트는 Windows, Mac OS X, Linux 플랫폼의 AnyConnect Secure Mobility에 대한 정보를 제공합니다.

참고 AnyConnect 릴리스 4.4.x는 모든 버그 4.x의 유지 보수 경로입니다. AnyConnect 4.0, 4.1, 4.2, 4.3 고객은 향후 결함 픽스를 이용하려면 AnyConnect 4.4.x로 업그레이드해야 합니다. AnyConnect 4.0.x, 4.1.x, 4.2.x, 4.3.x에서 발견된 결함은 AnyConnect 4.4.x 유지 보수 릴리스에서만 해결됩니다.

AnyConnect 최신 버전 다운로드

시작하기 전에

AnyConnect의 최신 버전을 다운로드하려면 Cisco.com에 등록된 사용자여야 합니다.

SUMMARY STEPS

1. 이 링크를 따라 Cisco AnyConnect Secure Mobility Client 제품 지원 페이지로 이동합니다.
2. Cisco.com에 로그인합니다.
3. **Download Software(**소프트웨어 다운로드**)**를 클릭합니다.
4. **Latest Releases(**최신 릴리스**)** 폴더를 확장하고 최신 릴리스가 아직 선택되지 않은 경우 최신 릴리스를 클릭합니다.
5. 다음 방법 중 하나를 사용하여 AnyConnect 패키지를 다운로드합니다.
   - 단일 패키지를 다운로드하려면 다운로드할 패키지를 찾고 **Download(**다운로드**)**를 클릭합니다.
   - 여러 패키지를 다운로드하려면 패키지 행에서 **Add to cart(**카트에 추가**)**를 클릭한 다음 Download Software(소프트웨어 다운로드) 페이지의 상단에서 **Download Cart(**카트 다운로드**)**를 클릭합니다.
6. Cisco 라이선스 계약서가 표시되면 내용을 읽고 동의합니다.
7. 다운로드 항목을 저장할 로컬 디렉터리를 선택하고 **Save(**저장**)**를 클릭합니다.
8. Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.x를 참조하십시오.

DETAILED STEPS

단계 **1** 이 링크를 따라 Cisco AnyConnect Secure Mobility Client 제품 지원 페이지로 이동합니다. http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html.

단계 **2** Cisco.com에 로그인합니다.

단계 **3** **Download Software(**소프트웨어 다운로드**)**를 클릭합니다.

단계 **4** **Latest Releases(**최신 릴리스**)** 폴더를 확장하고 최신 릴리스가 아직 선택되지 않은 경우 최신 릴리스를 클릭합니다.

단계 **5** 다음 방법 중 하나를 사용하여 AnyConnect 패키지를 다운로드합니다.

- 단일 패키지를 다운로드하려면 다운로드할 패키지를 찾고 **Download(**다운로드**)**를 클릭합니다.
- 여러 패키지를 다운로드하려면 패키지 행에서 **Add to cart(**카트에 추가**)**를 클릭한 다음 Download Software(소프트웨어 다운로드) 페이지의 상단에서 **Download Cart(**카트 다운로드**)**를 클릭합니다.

단계 **6** Cisco 라이선스 계약서가 표시되면 내용을 읽고 동의합니다.

단계 **7** 다운로드 항목을 저장할 로컬 디렉터리를 선택하고 **Save(**저장**)**를 클릭합니다.

단계 **8** Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.x를 참조하십시오.

웹 구축용 AnyConnect 패키지 파일 이름

OS	AnyConnect 웹 구축 패키지 이름
Windows	anyconnect-win-*version*-webdeploy-k9.pkg
Mac OS X	anyconnect-macos-*version*-webdeploy-k9.pkg
Linux(64비트)	anyconnect-linux64-*version*-webdeploy-k9.pkg

사전 구축용 AnyConnect 패키지 파일 이름

OS	AnyConnect 사전 구축 패키지 이름
Windows	anyconnect-win-*version*-predeploy-k9.zip
Mac OS X	anyconnect-macos-*version*-predeploy-k9.dmg
Linux(64비트)	anyconnect-linux64-*version*-predeploy-k9.tar.gz

AnyConnect에 기능을 추가하는 데 도움이 되는 다른 파일도 다운로드할 수 있습니다.

AnyConnect 4.4.03034 새 기능

AnyConnect 4.4.03034는 다음 개선 기능이 포함되고 AnyConnect 4.4.03034, 32 페이지에 설명된 결함을 해결하는 주요 릴리스입니다.

- NVM(Network Visibility Module)이 이제 Linux에서 지원되지만, 이를 사용하려면 우선 커널 드라이버 프레임워크를 설치해야 합니다. AnyConnect Kernel Module을 사전 구축하거나 대상에서 드라이버를 구축하도록 선택할 수 있습니다. 커널 모듈을 사전 구축하거나 대상에서 구축하는 경우에 상관없이, 다음 방법으로 대상 디바이스를 준비해야 합니다.
  - GNU Make Utility가 설치되었는지 확인합니다.
  - 커널 헤더 패키지를 설치합니다.

    RHEL의 경우 **kernel-devel-$(uname -r)** 패키지(예: kernel-devel-2.6.32-642.13.1.el6.x86_64)를 설치합니다.

    Ubuntu의 경우 **linux-headers-$(uname -r)** 패키지(예: linux-headers-4.2.0-27-generic)를 설치합니다.
  - GCC 컴파일러가 설치되었는지 확인합니다. 설치된 GCC 컴파일러의 *major.minor* 버전은 커널이 구축된 GCC 버전과 일치해야 합니다. /proc/version 파일에서 이를 확인할 수 있습니다.

자세한 내용은 AnyConnect 관리자 설명서를 참조하십시오. http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html

- 종속 포털 탐지 및 신뢰할 수 있는 네트워크 탐지가 이제 Linux 운영 체제에서 지원됩니다.
- 이 AnyConnect 4.4.03034 릴리스에서는 이제 LittleSnitch가 Mac OS X의 NVM과 호환됩니다.

AnyConnect 4.4.02039 새 기능

AnyConnect 4.4.02039는 다음 개선 기능이 포함되고 AnyConnect 4.4.02039, 34 페이지에 설명된 결함을 해결하는 주요 릴리스입니다.

AnyConnect 4.4.02034 새 기능

AnyConnect 4.4.02034는 다음 개선 기능이 포함되고 AnyConnect 4.4.02034, 34 페이지에 설명된 결함을 해결하는 주요 릴리스입니다.

AnyConnect 4.4.01054 새 기능

AnyConnect 4.4.01054는 다음 기능 및 개선 기능이 포함되고 AnyConnect 4.4.01054, 35 페이지에 설명된 결함을 해결하는 주요 릴리스입니다.

- ISE Posture의 개선 기능

참고 이러한 ISE Posture 기능을 사용하려면 ISE 2.2(이상 버전)가 필요합니다.

ISE 컨피그레이션에 대한 자세한 내용은 Cisco Identity Services Engine 관리 가이드, 릴리스 2.2를 참조하십시오.

  - 상태용 Stealth Agent — (Windows 및 Mac에만 해당) ISE Posture를 AnyConnect UI 내에서 숨겨진 서비스로 실행할 수 있습니다. 예를 들어, AnyConnect Stealth 상태 에이전트는 최종 사용자 클라이언트에서 시스템 스캔 타일 및 알림을 숨깁니다.
  - 지속적인 엔드포인트 모니터링 — 설치된 애플리케이션 및 실행 중인 애플리케이션을 모니터링하여 엔드포인트에서 동적 변경 사항을 관찰할 수 있도록 합니다.
  - 차세대 프로비저닝 및 검색 — ISE에서 AnyConnect 소프트웨어를 구축할 수 있는 추가적인 비 URL 리디렉션 기반 옵션을 제공할 뿐만 아니라, ISE 통신에 대한 AnyConnect의 추가적인 복원력도 제공합니다(서드파티 네트워크 인프라로 컴플라이언스 플로우를 지원할 수 있는 기능 포함).
  - 애플리케이션 삭제 및 제거 기능 — 선택한 애플리케이션에 정책 작업을 적용하거나 소프트웨어 라이선스 사용량을 줄일 수 있는 기능을 제공합니다.
  - 엔드포인트 상황 가시성 — UDID(Unique Identifier, 고유 식별자)를 추가하여 MAC 주소에만 의존하는 대신 특정 엔드포인트를 식별합니다.

- 추가적인 상황 확인 — (Windows 및 Mac에만 해당) 서드파티 및 기본 OS 방화벽 상태, 그리고 자동 치료를 확인합니다.

- OpenDNS Umbrella와 관련된 브랜드 이름이 변경되었습니다. 몇 가지 예를 들면 다음과 같습니다.
  - OpenDNS Umbrella가 이제 Cisco Umbrella로 변경되었습니다.
  - OpenDNS 글로벌 네트워크가 이제 Cisco Umbrella 글로벌 네트워크로 변경되었습니다.
  - Umbrella 가상 어플라이언스가 이제 Cisco Umbrella 가상 어플라이언스로 변경되었습니다.
  - OpenDNS Umbrella 로밍 클라이언트가 이제 Cisco Umbrella 로밍 클라이언트로 변경되었습니다.

AnyConnect 4.4.00243 새 기능

AnyConnect 4.4.00243은 다음 기능 및 개선 기능이 포함되고 AnyConnect 4.4.00243, 37 페이지에 설명된 결함을 해결하는 주요 릴리스입니다.

- SAML 2.0 SSO(ASA 릴리스 9.7.1과 통합됨) — SAML을 통해 더욱 폭넓은 웹 기반 인증을 지원합니다. SAML을 초기 SSO(Single-Signon) 세션 인증에 사용할 수 있습니다. 재연결하는 동안, 원활한 재연결이 중단될 수 있으므로 AnyConnect는 SAML 프로세스를 다시 진행하지 않습니다. 사용자가 브라우저를 사용하여 IdP에서 로그아웃할 경우에도 AnyConnect 세션은 그대로 유지됩니다. SAML 기능을 사용하려면 Apex 라이선스가 있어야 합니다.
- 다중 인증서 인증(ASA 릴리스 9.7.1과 통합됨) — Windows에서는 VPN 클라이언트 프로파일에서 사용할 AnyConnect용 인증서 저장소를 제공합니다. 이제 다중 인증서 인증을 조합하고 보안 게이트웨이를 구성하여 선택한 다중 인증서 인증 중 어떤 인증이 특정 VPN 연결에 허용되는지 클라이언트에 지시할 수 있습니다.
- 연결 시간 초과 시 보안 향상 — ASA에서 vpn-session-timeout 및 vpn-session-timeout alert-interval 설정을 사용하면 세션 제한이 초과된 경우 AnyConnect Secure Mobility Client의 최종 사용자에게 세션 만료 알림이 전송됩니다. "Your connection will soon exceed the session time limit. A new connection will be necessary(연결의 세션 시간 제한이 곧 초과됩니다. 새로 연결해야 합니다)"라는 내용의 UI 메시지가 표시되므로, VPN에서 로그아웃하지 않고도 상황을 바로잡을 수 있습니다. 이 설정 조정에 대한 자세한 내용은 여기(http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-groups.html)에서 **Specify the Maximum VPN Connection Time in Group Policy(**그룹 정책에서 최대 **VPN** 연결 시간 지정**)** 섹션을 참조하십시오.

  참고 이러한 알림을 표시하려면 **Show Connection Notices(**연결 알림 표시**)**를 AnyConnect 기본 설정으로 활성화해야 할 수 있습니다.

- DHCP 서버 경로 제어 — Windows에서 그룹 정책 맞춤설정 속성을 설정하여 DHCP 공용 서버 경로 만들기를 제어할 수 있습니다. 터널 설정 시 공용 DHCP 서버 경로를 만들지 않으려면 no-dhcp-server-route 맞춤설정 속성이 있어야 하며 *true*로 설정해야 합니다.

- 추가 IPv6 구현 — IPv6 연결은 단일 또는 이중 스택 네트워크에서 안정적이며, 사용자는 연결에 사용된 기본 및 보조 IP 프로토콜을 제어할 수 있습니다. IPv6에서 IPv4로 마이그레이션하거나 그 반대일 경우, 원활하게 재연결되며 터널 연결이 끊어진 경우 두 프로토콜 간에 대체 시스템이 작동해야 합니다. IPv6을 위한 IKEv2 터널 지원이 추가되었습니다.
- Network Visibility Module 개선 기능 —
  - 광범위한 데이터 수집으로 단순히 모든 것을 제외하는 것이 아니라 익명화에 대한 해싱 추가 제공
  - Windows, 64비트 Windows, Mac OS X에서 Java를 컨테이너로서 지원
  - 최대 크기 및 기간을 설정하는 캐시 컨피그레이션
  - 사용자가 구성하는 간격에 따라 플로우(예: 서버 연결 또는 다운로드)를 파악하는 주기적인 플로우 보고 기능
- Windows 서명 확인 업데이트 — Cisco에서 제공한 변형만 ASA 또는 ISE에 적용됩니다. 고객이 제공한 변형(Cisco에서 서명하지 않은 변형)은 작동하지 않습니다. OOB(Out of Band) 방법을 통해 고유한 변형을 적용할 수 있습니다.

Umbrella 로밍 보안 플러그인과 관련된 추가 버그 픽스

- 등록이 실패할 경우, 플러그인은 올바른 정책 없이 DNS 보호를 적용하게 될 수 있습니다.
- (Windows 10에만 해당) 시스템에서 네트워크 어댑터가 올바른 우선 순위 순서로 반환되지 않습니다.
- 클라우드 API 확장성이 지원되어 Umbrella 백엔드 클라우드 인프라에서 Umbrella 로밍 플러그인의 로드가 감소합니다.

참고 Cisco에서는 Umbrella 로밍 플러그인에서 도메인 검색 접미사를 올바르게 가져올 수 없어 로컬 도메인 확인 문제를 일으키는 시나리오를 조사하고 있는 중입니다.

Mac OS X 픽스

- (CSCvb49067) IPv6 네트워크에서 Umbrella 보호 상태가 열림
- Umbrella 플러그인 등록 중 엔드포인트 호스트 이름을 검색하는 데 오류가 발생하는 문제
- 클라우드 API 확장성이 지원되어 Umbrella 백엔드 클라우드 인프라에서 Umbrella 로밍 플러그인의 로드가 감소

중요한 상호 운용성 고려 사항

ISE 및 ASA 헤드엔드가 함께 있는 경우

- 클라이언트 상태에 ISE와 ASA를 모두 사용할 경우, 두 헤드엔드에서 프로파일이 모두 일치해야 합니다.
- AnyConnect는 NAC Agent가 엔드포인트에 대해 프로비저닝된 경우 ISE 1.3 서버를 무시합니다.
- Cisco NAC Agent 및 VPN Posture(HostScan) 모듈이 클라이언트에 모두 설치된 경우, 상태 충돌을 방지하려면 Cisco NAC Agent는 최소 4.9.4.3 이상 버전이어야 합니다.
- NAC Agent는 AnyConnect가 ISE에서 엔드포인트에 대해 프로비저닝된 경우 ISE 1.3 서버를 무시합니다.

시스템 요구 사항

이 섹션에서는 이번 릴리스의 관리 및 엔드포인트 요건에 대해 알아봅니다. 엔드포인트 OS 지원 및 각 기능의 라이선스 요건에 대한 내용은 AnyConnect Secure Mobility Client 기능, 라이선스, OS를 참조하십시오.

Cisco에서는 다른 VPN 서드파티 클라이언트와의 호환성을 보장할 수 없습니다.

AnyConnect 프로파일 편집기의 변경 사항

프로파일 편집기를 설치하려면 32비트 버전의 Java 6 이상을 설치해야 합니다.

AnyConnect 용 ISE 요건

ISE 릴리스 요건

- ISE 1.3은 AnyConnect 소프트웨어를 엔드포인트에 구축하고, AnyConnect 4.0 이상 버전의 새 ISE Posture 모듈을 사용하는 엔드포인트의 상태를 확인할 수 있는 최소 릴리스입니다.
- ISE 1.3은 AnyConnect 릴리스 4.0 이상만 구축할 수 있습니다. 이전 버전의 AnyConnect 릴리스는 ASA에서 웹 구축하거나, SMS를 통해 사전 구축하거나, 수동으로 구축해야 합니다.

ISE 라이선싱 요건

ISE 헤드엔드에서 AnyConnect를 구축하고 ISE Posture 모듈을 사용하려면 ISE 관리 노드에 Cisco ISE Apex 라이선스가 필요합니다. ISE 라이선스에 대한 자세한 내용은 Cisco Identity Services Engine 관리 설명서, 릴리스 2.0의 *Cisco ISE* 라이선스 장을 참조하십시오.

AnyConnect용 ASA 요건

ASA 릴리스 요건

- NVM을 사용하려면 ASDM 7.5.1로 업그레이드해야 합니다.
- AMP Enabler를 사용하려면 ASDM 7.4.2로 업그레이드해야 합니다.
- TLS 1.2를 사용하려면 ASA 9.3(2)로 업그레이드해야 합니다.
- 다음 기능을 사용하려면 ASA 9.2(1)로 업그레이드해야 합니다.
  - VPN을 통한 ISE Posture
  - AnyConnect 4.x의 ISE 구축
  - ASA에서의 CoA(Change of Authorization)는 이 버전 이상에서 지원됩니다.
- 다음 기능을 사용하려면 ASA 9.0으로 업그레이드해야 합니다.
  - IPv6 지원
  - Cisco Next Generation Encryption "Suite-B" 보안
  - AnyConnect 클라이언트 지연 업그레이드
- 다음을 수행하려면 ASA 8.4(1) 이상을 사용해야 합니다.
  - IKEv2 사용
  - ASDM을 사용하여 비 VPN 클라이언트 프로파일(예: Network Access Manager, Web Security 또는 텔레메트리) 수정
  - Cisco IronPort Web Security Appliance에서 지원되는 서비스 사용. 이러한 서비스를 사용하면 제한적 사용 정책을 시행하고, 모든 HTTP 및 HTTPS 요청을 허용 또는 거부하여 안전하지 않은 것으로 확인된 웹 사이트로부터 엔드포인트를 보호할 수 있습니다.
  - 방화벽 규칙 구축. 상시 연결 VPN을 구축할 경우, 스플릿 터널링을 활성화하고 로컬 인쇄 및 테더링 모바일 디바이스에 대한 네트워크 액세스를 제한하는 방화벽 규칙을 구성할 수 있습니다.
  - 상시 연결 VPN 구축에서 검증된 VPN 사용자를 제외하는 동적 액세스 정책 또는 그룹 정책 구성
  - AnyConnect 세션이 격리된 경우 AnyConnect GUI에 메시지가 표시되도록 동적 액세스 정책 구성

ASA 메모리 요건

주의 AnyConnect 4.0 이상을 사용하는 모든 ASA 5500 모델의 최소 권장 플래시 메모리는 512MB입니다. 이 메모리를 사용하여 여러 엔드포인트 운영 체제를 호스팅하고 ASA에서 로깅 및 디버깅을 활성화할 수 있습니다.

ASA 5505(최대 128MB)의 플래시 크기 제한으로 인해, AnyConnect 패키지의 일부 순열은 이 모델에서 로드할 수 없습니다. AnyConnect를 올바르게 로드하려면 사용 가능한 플래시 크기에 맞을 때까지 패키지 크기를 줄여야 합니다(예: OS 감소, Host Scan 제외 등).

AnyConnect 설치 또는 업그레이드를 진행하기 전에 사용 가능한 공간을 확인합니다. 다음 방법 중 하나를 사용하여 이를 확인할 수 있습니다.

- CLI — **show memory** 명령을 입력합니다.

```
asa3# show memory
Free memory:        304701712 bytes (57%)
Used memory:        232169200 bytes (43%)
-------------      ----------------
Total memory:       536870912 bytes (100%)
```

- ASDM — Tools(툴) > File Management(파일 관리)를 선택합니다. File Management(파일 관리) 창에 플래시 공간이 표시됩니다.

ASA에 기본 내장형 플래시 메모리 또는 기본 DRAM(캐시 메모리용)의 용량만 있을 경우 여러 AnyConnect 클라이언트 패키지를 ASA에 저장하고 로드하면서 문제가 생길 가능성이 있습니다. 플래시에 패키지 파일을 보관하기 위한 충분한 공간을 갖추고 있는 경우에도, ASA에서 클라이언트 이미지의 압축을 풀고 로드할 때 캐시 메모리가 모두 소진될 수 있습니다. ASA 메모리 요건 및 ASA 메모리 업그레이드에 대한 자세한 내용은 Cisco ASA 5500 Series의 최신 릴리스 노트를 참조하십시오.

VPN Posture와 Hostscan 상호 운용성

VPN Posture(HostScan) 모듈은 ASA에 대해 호스트에 설치된 운영 체제, 안티바이러스, 안티스파이웨어, 방화벽 소프트웨어를 식별할 수 있는 기능을 Cisco AnyConnect Secure Mobility Client에 제공합니다.

VPN Posture(HostScan) 모듈이 이러한 정보를 수집하려면 Hostscan이 필요합니다. 자체 소프트웨어 패키지로 제공되는 Hostscan은 새로운 운영 체제, 안티 바이러스, 안티스파이웨어, 방화벽 소프트웨어 정보와 함께 주기적으로 업데이트됩니다. 일반적으로는 가장 최신 버전의 HostScan(AnyConnect 버전과 동일)을 실행하는 것이 좋습니다.

AnyConnect 4.4.x는 HostScan 4.3.05017 이전의 HostScan 릴리스와 호환되지 않습니다. 그러나 AnyConnect 4.4.x는 HostScan 4.3.05017 이하 버전과 호환되며, HostScan 4.3.05017(또는 HostScan 4.3.x 릴리스 이후)을 ASDM에서 HostScan 이미지로 사용해야 합니다(Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Secure Desktop Manager > Host Scan image(Host Scan 이미지)).

cisco.com에서는 안티바이러스, 안티스파이웨어, 방화벽 애플리케이션 목록을 제공합니다. 지원 차트는 Firefox 브라우저를 사용했을 때 가장 쉽게 열립니다. Internet Explorer를 사용할 경우 파일을 컴퓨터에 다운로드하고 파일 확장자를 `.zip`에서 `.xlsm`으로 변경합니다. Microsoft Excel, Microsoft Excel 뷰어 또는 Open Office에서 파일을 열 수 있습니다.

참고 AnyConnect를 호환되지 않는 버전의 HostScan과 사용할 경우 VPN 연결을 설정할 수 없습니다. 또한, HostScan과 ISE Posture를 함께 사용하는 것은 바람직하지 않습니다. 서로 다른 두 가지 상태 에이전트를 함께 실행할 경우 예기치 않은 결과가 발생합니다.

ISE Posture Compliance 모듈

ISE Posture Compliance 모듈에는 ISE Posture에 대해 지원되는 안티바이러스, 안티스파이웨어, 방화벽 목록이 포함됩니다. HostScan 목록은 벤더별로 구성되지만 ISE Posture 목록은 제품 유형별로 구성됩니다. 헤드엔드(ISE 또는 ASA)의 버전 번호가 엔드포인트의 버전보다 클 경우, OPSWAT가 업데이트됩니다. 이러한 업그레이드는 필수이며 최종 사용자의 작업 없이 자동으로 수행됩니다.

라이브러리(zip 파일) 내에 있는 이러한 개별 파일은 OPSWAT, Inc.에서 디지털 서명하며 라이브러리 자체는 Cisco 인증서로 코드 서명한 단일한 자동 압축 풀기 실행 파일로 패키지됩니다. 다음 위치에서 Microsoft Excel, Microsoft Excel 뷰어 또는 OpenOffice를 사용하여 차트를 볼 수 있습니다.

AnyConnect의 IOS 지원

Cisco에서는 IOS Release 15.1(2)T 기능에 대한 AnyConnect VPN 액세스를 보안 게이트웨이로 지원하지만, IOS 릴리스 15.1(2)T에서는 현재 다음과 같은 AnyConnect 기능을 지원하지 않습니다.

- 사후 로그인 상시 연결 VPN
- 연결 실패 정책
- 로컬 프린터 및 테더링 디바이스 액세스를 제공하는 클라이언트 방화벽
- 최적의 게이트웨이 선별
- 격리
- AnyConnect 프로파일 편집기

AnyConnect VPN의 IOS 지원 제한에 대한 자세한 내용은 Cisco IOS SSL VPN에서 지원되지 않는 기능을 참조하십시오.

자세한 IOS 기능 지원 정보는 http://www.cisco.com/go/fn을 참조하십시오.

AnyConnect가 지원되는 운영 체제

Cisco AnyConnect Secure Mobility Client는 포함된 해당 모듈에 대해 다음 운영 체제를 지원합니다.

지원되는 운영 체제	VPN Client	Network Access Manager	Cloud Web Security	VPN [illegible]	ISE 상태	DART	고객 경험 피드백	Network Visibility Module	AMP Enabler	Umbrella 로밍 보안
Windows 7 SP1, 8, 8.1, 10 x86(32비트) 및 x64(64비트)	예	예	예	예	예	예	예	예	예	예

지원되는 운영 체제	VPN Client	Network Access Manager	Cloud Web Security	VPN PoSture (HostScan)	ISE 상태	DART	고객 경험 피드백	Network Visibility Module	AMP Enabler	Umbrella 로밍 보안
Mac OS X 10.10, 10.11 및 10.12	예	아니요	예	예	예	예	예	예	예	예
Linux Red Hat 6, 7 및 Ubuntu 12.04 (LTS), 14.04(LTS), 16.04(LTS)(64비트 전용)	예	아니요	아니요	예	아니요	예	예	아니요	아니요	아니요

참고 위 목록에 있는 버전과 다른 버전도 작동 가능할 수 있으나, Cisco에서는 위 목록 이외의 다른 버전에서는 전체 테스트를 수행하지 않았습니다.

Microsoft Windows 용 AnyConnect 지원

Windows 요건

- Pentium급 이상 프로세서
- 100MB 하드 디스크 공간
- Microsoft 설치 프로그램, 버전 3.1
- 이전 Windows 릴리스에서 Windows 8.1로 업그레이드할 경우, Windows 업그레이드가 완료되면 AnyConnect를 제거하고 다시 설치해야 합니다.
- Windows XP에서 이후 버전의 Windows 릴리스로 업그레이드할 경우, 업그레이드 동안 Cisco AnyConnect 가상 어댑터가 유지되지 않으므로 클린 설치를 수행해야 합니다. 수동으로 AnyConnect를 제거하고 Windows를 업그레이드한 다음, 수동으로 또는 WebLaunch를 통해 AnyConnect를 다시 설치합니다.
- WebLaunch로 AnyConnect를 시작하려면 32비트 버전 Firefox 3.0+을 사용하고 ActiveX를 활성화하거나 Sun JRE 1.4+를 설치해야 합니다.
- Windows 8 또는 8.1을 사용할 경우 ASDM 버전 7.02 이상이 필요합니다.

Windows 제한 사항

- Windows RT에서는 AnyConnect가 지원되지 않습니다. 이 기능을 수행할 수 있는 API가 운영 체제에서 제공되지 않습니다. Cisco에서는 이 문제에 대해 Microsoft에 공개 요청을 한 상태입니다. 이 기능을 사용하려는 사용자는 Microsoft에 문의하여 문제 사항을 전달해야 합니다.

- 기타 서드파티 제품이 Windows 8과 호환되지 않을 경우 AnyConnect가 무선 네트워크를 통해 VPN 연결을 설정할 수 없습니다. 이 문제의 두 가지 예는 다음과 같습니다.
  - Wireshark로 배포된 WinPcap 서비스 "Remote Packet Capture Protocol v.0 (experimental)"이 Windows 8에서 지원되지 않습니다.

    이 문제를 해결하려면 Wireshark를 제거하거나 WinPcap 서비스를 비활성화한 후, Windows 8 컴퓨터를 재부팅하고 AnyConnect 연결을 다시 시도하십시오.
  - Windows 8을 지원하지 않는 구형 무선 카드 또는 무선 카드 드라이버가 있을 경우 AnyConnect가 VPN 연결을 설정할 수 없습니다.

    이 문제를 해결하려면 Windows 8을 지원하는 최신 무선 네트워크 카드 또는 드라이버가 Windows 8 컴퓨터에 설치되어 있는지 확인하십시오.
- AnyConnect는 Windows 8에 구축된 Metro 설계 언어인 새로운 UI 프레임워크와 통합되지 않으나, AnyConnect는 Windows 8에서 데스크톱 모드로 실행됩니다.
- HP Protect 툴은 Windows 8.x에 설치된 AnyConnect에서 구동되지 않습니다.
- Windows 2008은 지원되지 않으나, 이 OS에서 AnyConnect를 설치할 수는 있습니다. 또한, Windows Server 2008 R2에는 선택적 SysWow64 구성 요소가 필요합니다.
- 대기 모드를 지원하는 시스템에서 Network Access Manager를 사용할 경우, 기본 Windows 8.x 연결 타이머 값(5초)을 사용하는 것이 좋습니다. Windows의 검사 목록이 예상보다 짧을 경우, 연결 타이머를 늘려 드라이버가 네트워크 검사를 완료하고 검사 목록을 채울 수 있도록 하십시오.

Windows 지침

- 클라이언트 시스템의 드라이버가 Windows 7 또는 8에서 지원되는지 확인합니다. 지원되지 않는 드라이버는 일시적인 연결 문제가 발생할 수 있습니다.
- Network Access Manager의 경우, Microsoft KB 2743127에 설명된 레지스트리 픽스를 클라이언트 데스크톱에 적용하지 않는 한 Windows 8 또는 10/Server 2012에서 컴퓨터 비밀번호를 사용한 컴퓨터 인증이 실행되지 않습니다. 이 픽스에는 DWORD 값인 LsaAllowReturningUnencryptedSecrets를 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa 레지스트리 키에 추가하고 이 값을 1로 설정하는 작업이 포함됩니다. 이렇게 변경하면 LSA(Local Security Authority)가 Cisco Network Access Manager 같은 클라이언트에 컴퓨터 비밀번호를 제공할 수 있게 됩니다. 이는 Windows 8 또는 10/Server 2012의 강화된 기본 보안 설정과 관련이 있습니다. 컴퓨터 인증서를 사용하는 컴퓨터 인증에는 이러한 변경 사항이 필요하지 않으며 이전 Windows 8 운영 체제와 같은 방식으로 작동합니다.

참고 컴퓨터 인증은 사용자가 로그인하기 전에 클라이언트 데스크톱이 네트워크에 대한 인증을 받을 수 있도록 합니다. 이 시간 동안 관리자는 이 클라이언트 컴퓨터에 대해 예약된 관리 작업을 수행할 수 있습니다. RADIUS 서버가 특정 클라이언트에 대해 사용자 및 컴퓨터를 모두 인증할 수 있는 EAP 체이닝 기능에도 컴퓨터 인증이 필요합니다. 이를 통해 회사 자산을 식별하고 적절한 액세스 정책을 적용할 수 있습니다. 예를 들어 이 디바이스가 개인 자산(PC/노트북 컴퓨터/태블릿)이고 기업 자격 증명을 사용하는 경우, 엔드포인트에서 컴퓨터 인증은 실패하지만 사용자 인증은 성공하며 적절한 네트워크 액세스 제한이 사용자의 네트워크 연결에 적용됩니다.

- Windows 8의 Preferences(기본 설정) > VPN > Statistics(통계) 탭에서 Export Stats(통계 내보내기) 버튼을 눌러 파일을 데스크톱에 저장합니다. 다른 버전의 Windows에서는 파일을 저장할 위치를 묻는 메시지가 표시됩니다.
- AnyConnect VPN은 WWAN 어댑터를 통해 Windows 7 이상 버전과 연결되는 3G 데이터 카드와 호환됩니다.

Linux용 AnyConnect 지원

Linux 요건

- x86 명령 집합
- 64비트 프로세서
- 32MB RAM.
- 20MB 하드 디스크 공간
- 설치에 필요한 Superuser(슈퍼 사용자) 권한
- libstdc++ 사용자는 libstdc++.so.6(GLIBCXX_3.4) 이상, 버전 4 이하를 보유해야 함
- Java 5(1.5) 이상 웹 설치가 가능한 유일한 버전은 Sun Java입니다. Sun Java를 설치하고 기본 패키지 대신 사용할 브라우저를 구성해야 합니다.
- zlib - SSL Deflate 압축 지원
- xterm - ASA 클라이언트리스 포털에서 WebLaunch를 통해 AnyConnect를 초기 구축하는 경우에만 필요합니다.
- gtk 2.0.0
- gdk 2.0.0
- libpango 1.0
- iptables 1.2.7a 이상
- 커널 2.4.21 또는 2.6과 함께 제공되는 tun 모듈

Mac OS X용 AnyConnect 지원

Mac OS X 요건

- AnyConnect에는 50MB의 하드 디스크 공간이 필요합니다.
- Mac OS X이 올바르게 작동하려면, AnyConnect에는 최소 1024 x 640픽셀의 디스플레이 해상도가 필요합니다.

Mac OS X 지침

- Mac OS X 10.8에는 시스템에서 어떤 애플리케이션을 실행할 수 있는지 제한하는 Gatekeeper라는 새로운 기능이 있습니다. 다음 위치에서 애플리케이션 다운로드를 허용하도록 선택할 수 있습니다.
  - Mac App Store
  - Mac App Store 및 확인된 개발자
  - 위치 무관

  기본 설정은 Mac App Store 및 확인된 개발자(서명된 애플리케이션)입니다. AnyConnect는 서명된 애플리케이션이지만 Apple 인증서를 사용하여 서명되지 않습니다. 이는 Anywhere 설정을 선택하거나, Ctrl 키를 누른 상태로 클릭하여 선택한 설정을 우회하고 사전 구축 설치에서 AnyConnect를 설치하고 실행해야 함을 의미합니다. 웹 구축하거나 AnyConnect를 이미 설치한 사용자에게는 영향을 미치지 않습니다. 자세한 내용은 http://www.apple.com/macosx/mountain-lion/security.html을 참조하십시오.

참고 웹 구동 또는 OS 업그레이드(예: 10.7~10.8)가 정상적으로 설치됩니다. 사전 구축 설치에만 Gatekeeper에 대한 추가 컨피그레이션이 필요합니다.

AnyConnect 라이선싱

최신 최종 사용자 라이선스 계약을 보려면 Cisco 최종 사용자 라이선스 계약, AnyConnect Secure Mobility Client, 릴리스 4.x를 참조하십시오.

Cisco의 오픈 소스 라이선싱 승인을 보려면 AnyConnect Secure Mobility Client에서 사용된 오픈 소스 소프트웨어를 참조하십시오.

ISE 헤드엔드에서 AnyConnect를 구축하고 ISE Posture 모듈을 사용하려면 ISE 관리 노드에 Cisco ISE Apex 라이선스가 필요합니다. ISE 라이선스에 대한 자세한 내용은 Cisco Identity Services Engine 관리 설명서, 릴리스 2.1의 *Cisco ISE* 라이선스 장을 참조하십시오.

ASA 헤드엔드에서 AnyConnect를 구축하고 VPN 및 VPN Posture(HostScan) 모듈을 사용하려면, AnyConnect 4.X Plus 또는 Apex 라이선스가 필요합니다. 평가판 라이선스가 제공되며 Cisco AnyConnect 주문 설명서를 참조하십시오.

AnyConnect 4.X Plus 및 Apex 라이선스 개요를 살펴보고 기능에서 사용되는 라이선스에 대한 설명을 보려면 AnyConnect Secure Mobility Client 기능, 라이선스, OS를 참조하십시오.

AnyConnect 설치 개요

AnyConnect 구축 시에는 AnyConnect 클라이언트 및 관련 파일을 설치, 구성 및 업그레이드합니다. Cisco AnyConnect Secure Mobility Client는 다음과 같은 방법으로 원격 사용자에게 배포할 수 있습니다.

- 사전 구축 - 엔터프라이즈 SMS(Software Management System, 소프트웨어 관리 시스템)를 사용하거나 최종 사용자가 신규 설치 및 업그레이드를 수행합니다.
- 웹 구축 - AnyConnect 패키지가 헤드엔드 즉 ASA 또는 ISE 서버에 업로드됩니다. 사용자가 ASA 또는 ISE에 연결할 때 AnyConnect는 클라이언트에 구축됩니다.
  - 신규 설치의 경우 사용자가 헤드엔드로 연결하여 AnyConnect 클라이언트를 다운로드합니다. 클라이언트는 수동 또는 자동(웹 실행)으로 설치됩니다.
  - AnyConnect가 이미 설치된 시스템에서 실행 중인 AnyConnect를 통해 또는 사용자를 ASA 클라이언트리스 포털로 디렉션하는 방법으로 업데이트가 수행됩니다.

AnyConnect를 구축할 때 VPN과 기타 기능을 구성하는 클라이언트 프로파일 및 추가 기능을 활성화하는 선택적 모듈을 포함할 수 있습니다. 다음 사항에 주의하십시오.

- 모든 AnyConnect 모듈 및 프로파일은 사전 구축할 수 있습니다. 사전 구축할 경우, 모듈 설치 순서 및 기타 세부사항에 각별한 주의를 기울여야 합니다.
- Customer Experience Feedback 모듈 및 VPN Posture 모듈에서 사용되는 Hostscan 패키지는 ISE에서 웹 구축할 수 없습니다.
- ISE Posture 모듈에서 사용된 Compliance 모듈은 ASA에서 웹 구축할 수 없습니다.

AnyConnect 모듈 구축에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.4를 참조하십시오.

참고 새 AnyConnect 패키지로 업그레이드할 경우 항상 CCO의 최신 릴리스로 현지화 MST 파일을 업데이트해야 합니다.

3.1 MR10 AnyConnect 클라이언트/비호환성 문제에서 업그레이드

AnyConnect 3.1.10010이 엔드포인트에 자동으로 구축되면, 호환되지 않는 AnyConnect 버전 4.0, 4.1, 4.1MR2, 4.2, 4.3으로 구성된 보안 게이트웨이에 연결할 수 없습니다. AnyConnect 3.1 MR10 버전에서 AnyConnect 4.1MR4(이상) 이외의 다른 버전 또는 3.1.10010 이상의 3.1 버전으로 업그레이드하려는 경우, 업그레이드할 수 없다는 알림이 표시됩니다.

자세한 내용은 CSCuv12386을 참조하십시오.

AnyConnect 3.0 이상 버전에서 업그레이드

AnyConnect Secure Mobility Client 릴리스 3.0 이상 버전에서 업그레이드할 경우, AnyConnect는 다음 작업을 수행합니다.

- 코어 클라이언트의 모든 이전 버전을 업그레이드하고 모든 VPN 컨피그레이션을 유지합니다.
- AnyConnect에서 사용된 Host Scan 파일을 업그레이드합니다.

AnyConnect 2.5 및 이전 버전에서 업그레이드

2.5.x 버전의 AnyConnect에서 업그레이드할 경우, AnyConnect Secure Mobility Client는 다음 작업을 수행합니다.

- 코어 클라이언트의 모든 이전 버전을 업그레이드하고 모든 VPN 컨피그레이션을 유지합니다.
- AnyConnect에서 사용된 Host Scan 파일을 업그레이드합니다.
- Network Access Manager를 설치할 경우, AnyConnect는 Network Access Manager에 사용할 모든 CSSC 5.x 컨피그레이션을 유지한 다음, CSSC 5.x를 제거합니다.
- Cisco IPsec VPN 클라이언트를 업그레이드하거나 제거하지 않습니다. 그러나 AnyConnect 클라이언트는 컴퓨터에서 IPsec VPN 클라이언트와 공존할 수 있습니다.
- 업그레이드되지 않으며 Cisco의 ScanSafe AnyWhere+와 공존할 수 없습니다. AnyConnect Secure Mobility Client를 설치하기 전에 AnyWhere+를 제거해야 합니다.

참고 레거시 Cisco VPN 클라이언트에서 업그레이드하는 경우, 물리적 어댑터의 MTU 값을 1300보다 낮춰야 했을 수 있습니다. AnyConnect를 사용할 때 최적의 성능을 실현하려면 각 어댑터의 MTU 값을 기본값(일반적으로 1500)으로 복원해야 합니다.

ASA 또는 WebLaunch를 사용하여 AnyConnect 2.2에서 업그레이드하는 방식은 지원되지 않습니다. AnyConnect 2.2를 제거한 다음 수동으로 또는 SMS를 사용하여 새 버전을 설치해야 합니다.

64비트 Windows에서 웹 기반 설치가 실패할 수 있는 문제

이 문제는 Windows 버전 7 및 8의 Internet Explorer 버전 10, 11에 적용됩니다.

Windows 레지스트리 항목 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth를 0으로 설정하면, AnyConnect 웹 구축이 진행되는 동안 Active X 문제가 발생합니다.

자세한 내용은 http://support.microsoft.com/kb/2716529를 참고하십시오.

해결책은 다음과 같습니다.

- 32비트 버전의 Internet Explorer를 실행합니다.
- 레지스트리 항목을 0이 아닌 값으로 수정하거나, 레지스트리에서 해당 값을 제거합니다.

참고 Windows 8의 경우, Windows 시작 화면에서 Internet Explorer를 시작하면 64비트 버전을 실행합니다. 데스크톱에서 시작하면 32비트 버전을 실행합니다.

AnyConnect 지원 정책

Cisco에서는 가장 최근의 4.x 릴리스를 기준으로만 픽스 및 개선 기능을 제공합니다. TAC 지원은 AnyConnect 4.x 릴리스 버전을 실행 중인 유효한 AnyConnect 4.x 약정/계약을 보유한 모든 고객에게 제공됩니다. 만료된 소프트웨어 버전에 문제가 발생한 경우, 현재 유지 보수 릴리스로 문제가 해결되는지 확인해볼 수 있습니다.

현재 픽스에서 Software Center 액세스는 AnyConnect 4.x 버전으로 제한됩니다. 구축하려는 버전이 향후에도 다운로드 가능한지 보장할 수 없으므로 구축에 필요한 모든 이미지를 다운로드하는 것이 좋습니다.

지침 및 제한 사항

Network Access Manager가 설치된 경우 Microsoft에서 Windows 10에 대한 업데이트를 차단함

Microsoft에서는 Network Access Manager가 설치된 경우 이전 버전의 Windows에 대한 업데이트를 차단하고 있으나, Windows 10 및 Creators Edition(RS2)까지 차단되었습니다. 이는 오류(Microsoft Sysdev 11911272) 때문이며, Creators Editor(RS2)로 업그레이드하려면 먼저 Network Access Manager 모듈을 제거해야 합니다. 업그레이드 후 모듈을 다시 설치할 수 있습니다. 이 오류에 대한 Microsoft의 픽스는 2017년 6월에 제공될 예정입니다.

Windows 10 Defender 오탐지 — Cisco AnyConnect 어댑터 문제

Windows 10 Creator Update(2017년 4월)로 업그레이드할 경우, AnyConnect 어댑터에 문제가 있다는 Windows Defender 메시지가 표시될 수 있습니다. Windows Defender에서는 Device Performance and Health(디바이스 성능 및 상태) 섹션에서 어댑터를 활성화하라는 메시지를 표시합니다. 그러나 실제로는 어댑터를 사용하고 있지 않을 경우 비활성화해야 하며 수동 조치를 취해서는 안 됩니다. 이 오탐지 오류는 Sysdev # 11295710으로 Microsoft에 보고되었습니다.

AnyConnect 4.4MR1(이상) 및 4.3MR5는 Windows 10 Creators Edition(RS2)과 호환됩니다.

AnyConnect와 Microsoft Windows 10의 호환성

AnyConnect 4.1MR4(4.1.04011) 이상 버전은 Windows 10 공식 릴리스와 호환됩니다. TAC(Technical Assistance Center) 지원은 2015년 7월 29일부터 시작되었습니다.

최상의 결과를 얻으려면, 즉 Windows 10 시스템에서 AnyConnect를 클린 설치하고 Windows 7/8/8.1에서 업그레이드하지 않는 것이 좋습니다. AnyConnect가 사전 설치된 Windows 7/8/8.1에서 업그레이드를 수행하려는 경우, 운영 체제를 업그레이드하기 전에 AnyConnect를 먼저 업그레이드해야 합니다. Windows 10으로 업그레이드하기 전에 Network Access Manager 모듈을 반드시 제거해야 합니다. 시

스템 업그레이드가 완료되면 시스템에서 Network Access Manager를 다시 설치할 수 있습니다. Windows 10으로 업그레이드한 후 AnyConnect를 완전히 제거하고 지원되는 버전 중 하나를 다시 설치할 수도 있습니다.

연결된 대기 상태에 대한 **Win32** 제한

AnyConnect는 Win32(Windows 저장소 아님) 애플리케이션이므로, 권한과 관련하여 Microsoft의 제한 사항이 적용됩니다. 따라서, AnyConnect는 Windows 8 이상 버전에서 연결된 대기(이벤트 중지 및 다시 시작) 상태에 대한 액세스 권한을 제공하지 않습니다.

새로운 **Split Include** 터널 동작**(CSCum90946)**

이전에는 split-include 네트워크가 로컬 서브넷의 수퍼넷일 경우, 로컬 서브넷과 정확히 일치하는 split-include 네트워크를 구성하지 않는 한 로컬 서브넷 트래픽이 터널링되지 않았습니다. 이제 CSCum90946이 해결됨에 따라, split-include 네트워크가 로컬 서브넷의 수퍼넷인 경우 access-list(ACE/ACL)에 split-include(0.0.0.0/32 또는 ::/128 거부)가 구성되어 있으면 로컬 서브넷 트래픽이 터널링됩니다.

split-include에 수퍼넷이 구성되어 있고 원하는 동작이 LocalLan 액세스를 허용하는 것일 때, 새 동작에는 다음 컨피그레이션이 필요합니다.

- access-list(ACE/ACL)에 수퍼넷에 대한 허용 작업과 0.0.0.0/32 또는 ::/128에 대한 거부 작업이 둘 다 포함되어야 합니다.
- AnyConnect 프로파일에서 로컬 LAN 액세스를 활성화합니다(프로파일 편집기의 Preferences Part 1(기본 설정 파트 1에서). (사용자가 제어 가능하도록 설정하는 옵션도 있습니다.)

Microsoft의 단계적인 **SHA-1** 지원 중단

2017년 2월 14일 이후부터는 SHA-1 인증서가 포함된 보안 게이트웨이 또는 SHA-1 중간 인증서가 포함된 인증서가 Windows Internet Explorer 11/Edge 브라우저 또는 Windows AnyConnect 엔드포인트에서 더 이상 유효한 인증서로 간주되지 않을 수 있습니다. 2017년 2월 14일 이후로 Windows 엔드포인트에서는 SHA-1 인증서 또는 중간 인증서가 포함된 보안 게이트웨이를 더 이상 신뢰할 수 있는 게이트웨이로 간주하지 않을 수 있습니다. 반드시 SHA-1 ID 인증서가 포함되지 않고 SHA-1 이외의 중간 인증서를 포함한 보안 게이트웨이를 사용하시기 바랍니다.

Microsoft에서는 원래 기록 및 날짜 계획을 수정했습니다. Microsoft에서는 현재 환경이 2017년 2월 변경 사항의 영향을 받는지 테스트하는 자세한 방법을 게시했습니다. Cisco에서는 SHA-1 보안 게이트웨이나 중간 인증서를 사용하거나 이전 버전의 AnyConnect를 실행할 경우 AnyConnect가 올바르게 작동할지 여부를 보장할 수 없습니다.

제공되는 모든 픽스를 제대로 적용하려면 반드시 AnyConnect의 최신 유지 보수 릴리스로 업데이트하는 것이 좋습니다. 유효한 AnyConnect Plus, Apex, VPN Only 약정/계약을 보유한 고객에게는 Cisco.com Software Center에서 AnyConnect 4.x 이상의 최신 업데이트 버전이 제공됩니다. AnyConnect Version 3.x는 더 이상 유지 보수가 제공되지 않으며 구축에 더 이상 사용할 수 없습니다.

참고 Microsoft의 단계적인 SHA-1 지원 중단에 따라, Cisco에서는 AnyConnect 4.3 및 4.4(이상) 릴리스가 계속 올바르게 작동하는지 확인했습니다. 장기적으로 Microsoft에서는 모든 상황에서 전체 Windows에 걸쳐 SHA-1을 신뢰하지 않을 것으로 예상되지만, 현재 공지에는 이에 대한 구체적인 정보나 날짜가 제공되지 않았습니다. 정확한 사용 중단 날짜가 고지되면, 언제라도 다수의 이전 버전 AnyConnect를 더 이상 구동하지 못할 수 있습니다. 자세한 내용은 Microsoft 공지를 참조하십시오.

SHA512 인증서를 인증에 사용할 경우 인증 실패

(Windows 7, 8, 8.1 사용자에 해당) 클라이언트가 SHA512 인증서를 인증에 사용할 경우 인증이 실패하며 클라이언트 로그에 해당 인증서가 사용 중이라고 표시되는 경우에도 마찬가지입니다. ASA 로그에는 AnyConnect에서 전송한 인증서가 없다고 올바르게 표시됩니다. 이러한 버전의 Windows에서는 TLS 1.2에서 SHA512 인증서 지원을 활성화해야 하며, 이는 기본적으로 지원되지 않습니다. 이러한 SHA512 인증서 지원을 활성화하는 방법에 대한 내용은 https://support.microsoft.com/en-us/kb/2973337을 참조하십시오.

RC4 TLS 암호 그룹이 더 이상 지원되지 않음

보안 정책 개선으로 인해 AnyConnect 릴리스 4.2.01035 이후 버전부터는 RC4 TLS 암호 그룹이 지원되지 않습니다.

OpenSSL 암호 그룹 변경

OpenSSL 표준 개발 팀에 따르면 일부 암호 그룹에 보안 침해가 발생한 것으로 확인되었으므로, AnyConnect 3.1.05187 이상에서는 해당 암호 그룹을 더 이상 지원하지 않습니다. 지원되지 않는 암호 그룹에는 DES-CBC-SHA, RC4-SHA, RC4-MD5가 포함됩니다.

이와 마찬가지로, Cisco의 암호화 툴킷에서는 RC4 암호에 대한 지원을 중지했습니다. 따라서, 3.1.13011 및 4.2.01035 이상 릴리스에서는 해당 암호가 삭제됩니다.

Mac OS X El Capitan 10.11에서 AnyConnect 지원

Cisco AnyConnect Secure Mobility Client는 Mac OS X El Capitan 10.11 운영 체제에서 지원됩니다.

ISE Posture에서 로그 추적 사용

새로 설치하면 ISE Posture 로그 추적 메시지가 정상적으로 표시됩니다. 그러나 ISE Posture 프로파일 편집기로 들어가 Enable Agent Log Trace file(에이전트 로그 추적 파일 활성화)을 0(비활성화)으로 변경할 경우, 정상적인 결과를 얻으려면 AnyConnect 서비스를 재시작해야 합니다.

Mac에서 ISE Posture와의 상호 운용성

Mac OS X 10.9 이상을 사용 중이고 ISE Posture를 사용하려는 경우, 문제를 방지하기 위해 다음 작업을 수행해야 할 수 있습니다.

- 상태 평가 도중 "failed to contact policy server(정책 서버에 연결 실패)" 오류를 방지하려면 인증서 유효성 검사를 끕니다.
- 종속 포털 애플리케이션을 비활성화합니다. 그렇지 않으면 검색 프로브가 차단되고, 애플리케이션이 사전 상태 ACL 상태로 남아 있습니다.

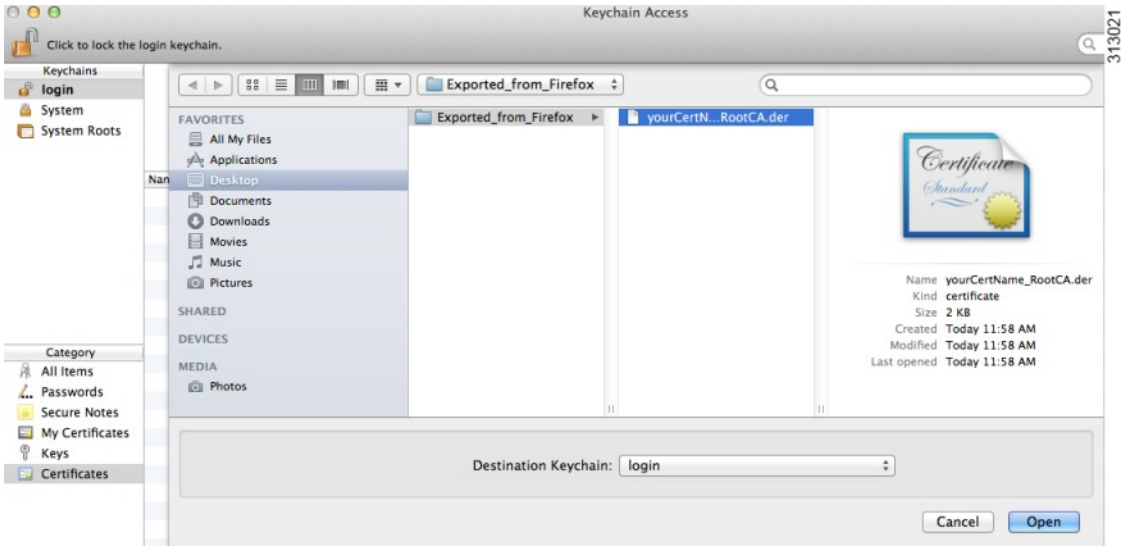
Mac OS X에서 Firefox 인증서 저장소가 지원되지 않음

Mac OS X의 Firefox 인증서 저장소는 사용자가 저장소의 콘텐츠를 변경할 수 있는 권한과 함께 저장됩니다. 이를 통해 무단 사용자 또는 프로세스가 합법적이지 않은 CA를 신뢰할 수 있는 루트 저장소에 추가할 수 있습니다. 따라서 AnyConnect에서는 서버 검증 또는 클라이언트 인증서에 Firefox 저장소를 더 이상 사용하지 않습니다.

필요한 경우, 사용자에게 Firefox 인증서 저장소에서 AnyConnect 인증서를 내보내는 방법과 해당 인증서를 Mac OS X 키 체인으로 가져오는 방법을 알려 주십시오. 다음 단계는 AnyConnect 사용자에게 안내하게 될 수 있는 내용의 예시입니다.

1. **Firefox > Preferences(**설정**) > Advanced(**고급**)**, Certificates(인증서) 탭으로 이동한 다음 **View Certificates(**인증서 보기**)**를 클릭합니다.
2. AnyConnect에 사용된 인증서를 선택하고 **Export(**내보내기**)**를 클릭합니다.

   AnyConnect 인증서는 Authorities(인증 기관) 범주 아래에 있습니다. 인증서 관리자를 확인합니다. 인증서 관리자는 Certificates(인증서) 또는 Servers(서버) 같은 다른 범주 아래에 있을 수 있습니다.
3. 인증서를 저장할 위치를 선택합니다(예: 데스크톱의 폴더).
4. 형식 풀다운 메뉴에서 **X.509 Certificate (DER)(X.509** 인증서**(DER))**를 선택합니다. 필요한 경우 인증서 이름에 .der 확장자를 추가합니다.

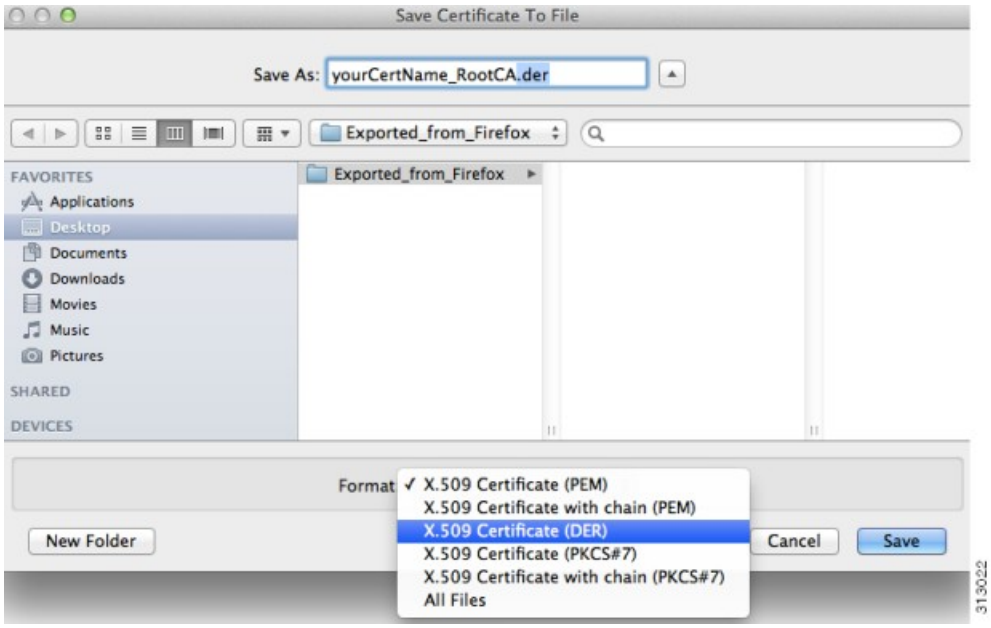


참고 AnyConnect 인증서가 두 개 이상이거나 개인 키가 사용/필요한 경우, 각 인증서에 위 프로세스를 반복합니다.

5 키 체인을 시작합니다. File(파일), Import Items(항목 가져오기)로 이동하고 Firefox에서 내보낸 인증서를 선택합니다.

Destination Keychain(대상 키 체인)에서 원하는 키 체인을 선택합니다. 회사에서는 이 예시에 사용된 로그인 키 체인과 다른 키 체인을 사용할 수 있습니다. 인증서 관리자에게 인증서에 어떤 키 체인을 가져와야 하는지 물어보십시오.

6 Destination Keychain(대상 키 체인)에서 원하는 키 체인을 선택합니다. 회사에서는 이 예시에 사용된 로그인 키 체인과 다른 키 체인을 사용할 수 있습니다. 인증서 관리자에게 인증서에 어떤 키 체인을 가져와야 하는지 물어보십시오.



7 AnyConnect에 추가 인증서가 사용되거나 필요한 경우 해당 인증서에 이전 단계를 반복합니다.

종속성 **libpangox**의 누락으로 **AnyConnect UI**가 실패함

여러 최신 Linux 배포에서 AnyConnect UI가 오류로 인해 시작되지 않을 수 있습니다.

```
error while loading shared libraries: libpangox-1.0.so.0: cannot open shared
object file: No such file or directory
```

누락된 라이브러리는 사용되지 않으며 더 이상 제공되지 않습니다. 이는 AnyConnect뿐만 아니라 다른 애플리케이션에도 영향을 미칩니다.

Pango에서는 다른 개발자가 구축한 호환 라이브러리 소스 코드를 릴리스했으며 이는 온라인에서 제공됩니다. 이 문제를 해결하려면 *pangox-compat-0.0.2-2.el7.x86_64.rpm* 또는 `pangox-compat-0.0.2-3.fc20.x86_64.rpm` 패키지를 찾아 설치합니다.

SSLv3로 인해 **Host Scan**이 작동하지 않음

(CSCue04930) ASDM에서 SSLv3 옵션 중 SSLv3만 선택하거나 Negotiate SSLv3(SSLv3 협상)을 선택한 경우(Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정) > 서버로 협상할 보안 어플라이언스의 SSL 버전), Host Scan이 작동하지 않습니다. ASDM에 관리자에게 알리는 경고 메시지가 표시됩니다.

수정된 **sysctl** 네트워크 설정으로 인한 문제

Apple의 Broadband Tuner 애플리케이션(2005)을 Mac OS X 10.9와 함께 사용할 경우, 해당 애플리케이션이 sysctl.conf의 네트워크 설정을 변경하는 경우가 있는 것으로 확인되었으며, 이로 인해 연결 문제가 발생할 수 있습니다. 이 애플리케이션은 Mac OS의 구형 버전용으로 설계된 것입니다. 현재 기본 OS 설정에서는 광대역 네트워크를 고려하는 것으로 예상되므로, 대부분의 사용자는 다른 조치를 취할 필요가 없습니다.

수정된 sysctl 설정과 함께 AnyConnect 3.1.04074를 실행할 경우 다음과 같은 메시지가 생성될 수 있습니다.

```
The VPN client driver encountered an error..please restart
```

확인 방법

sysctl 네트워크 설정이 문제의 원인인지 확인하려면 터미널 창을 열고 다음을 입력합니다.

```
sysctl -a | grep maxsockbuf
```

결과에 기본값인 8388608보다 작은 값이 포함된 경우, 아래 예시와 같이 표시됩니다.

```
kern.ipc.maxsockbuf: 512000
```

Apple의 Broadband Tuner 애플리케이션이 /etc/sysctl.conf에서 이 값을 덮어씁니다.

해결 방법

/etc/sysctl.conf를 수정하고 kern.ipc.maxsockbuf를 설정하는 행을 주석 처리한 다음, 컴퓨터를 리부팅합니다.

또는

Broadband Tuner 애플리케이션에서 설정한 것 이외의 맞춤설정이 없을 경우, sysctl.conf의 이름을 바꾸거나 삭제합니다.

Apple에서 이 문제를 알고 있으며 버그 ID: 15542576을 공개했습니다.

Safari의 **WebLaunch** 문제

Safari에서 WebLaunch를 사용하는 데 문제가 있습니다. OS X 10.9(Mavericks)에 제공되는 Safari 버전의 기본 보안 설정으로 인해 AnyConnect WebLaunch가 작동하지 않습니다. Safari에서 WebLaunch를 허용하도록 구성하려면 아래에 설명된 대로 ASA의 URL을 Unsafe Mode(비안전 모드)로 수정합니다.

1. **Safari** > **Preferences(**기본 설정**)** > **Security(**보안**)** > **Manage Website Settings(**웹 사이트 설정 관리**)**를 차례로 엽니다.
2. ASA를 클릭하고 Unsafe Mode(비안전 모드)에서 실행하도록 선택합니다.

활성 **X** 업그레이드로 인해 **WebLaunch**가 비활성화될 수 있음

ActiveX 컨트롤을 변경해야 할 필요가 없는 한, 제한된 사용자 어카운트로 WebLaunch를 통해 AnyConnect 소프트웨어의 자동 업그레이드를 수행할 수 있습니다.

보안 픽스 또는 새 기능의 추가로 인해 컨트롤을 변경해야 하는 경우가 가끔 있습니다.

제한된 사용자 어카운트에서 컨트롤을 업그레이드해야 할 경우, 관리자는 AnyConnect 사전 설치 프로그램, SMS, GPO 또는 기타 관리자 구축 방법을 사용하여 컨트롤을 구축해야 합니다.

Java 7 문제

Java 7은 AnyConnect Secure Mobility Client, Hostscan, CSD, 클라이언트리스 SSL VPN(WebVPN)에 문제를 초래할 수 있습니다. 문제 및 해결책에 대한 설명은 Security(보안) > Cisco Hostscan 아래에 게시된 Cisco 문서인 Troubleshooting Technote(트러블슈팅 기술문서)의 AnyConnect, CSD/Hostscan, WebVPN에 대한 Java 7 문제 - 트러블슈팅 설명서에서 제공됩니다.

Internet Explorer, Java 7, AnyConnect 3.1.1 상호 운용성

엔드포인트에 Java 7이 설치되어 있는 경우, Host Scan이 설치되어 있고 ASA에서 활성화된 경우, 그리고 AnyConnect 3.1.1이 설치되어 있고 ASA에서 활성화된 경우 사용자가 ASA에 연결하려고 하면 지원되는 버전의 Internet Explorer가 중단됩니다.

Active X 또는 Java 7 이하 버전이 설치된 경우에는 이러한 문제가 발생하지 않습니다. 이 문제를 방지하려면 엔드포인트에서 Java 7 이하의 지원되는 Java 버전을 사용하십시오.

확인하려면 Bug Toolkit 및 결함 CSCuc48299를 참조하십시오.

Tunnel All Networks(모든 네트워크 터널링)가 구성된 경우 암시적 DHCP 필터가 적용됨

Tunnel All Networks(모든 네트워크 터널링)가 구성된 경우 로컬 DHCP 트래픽을 투명하게 전송하기 위해 AnyConnect 클라이언트 연결 시 AnyConnect는 로컬 DHCP 서버에 특정 경로를 추가합니다. 또한, 이 경로에서 데이터 유출을 방지하기 위해 AnyConnect는 호스트 머신의 LAN 어댑터에 암시적 필터를 적용하여 해당 경로에 대해 DHCP 트래픽을 제외한 모든 트래픽을 차단합니다.

테더링 디바이스의 AnyConnect VPN

Cisco에서는 Bluetooth 또는 USB 테더링 Apple iPhone에서만 AnyConnect VPN 클라이언트를 검증했습니다. 다른 테더링 디바이스에서 제공하는 네트워크 연결은 구축 전에 AnyConnect VPN 클라이언트로 검증해야 합니다.

AnyConnect 스마트 카드 지원

AnyConnect는 다음 환경에서 스마트 카드가 제공된 자격 증명을 지원합니다.

- Windows7, Windows 8, Windows 10의 Microsoft CAPI 1.0 및 CAPI 2.0
- Mac OS X, 10.4 이상의 Tokend를 통한 키 체인

참고 AnyConnect는 Linux 또는 PKCS #11 디바이스에서는 스마트 카드를 지원하지 않습니다.

AnyConnect 가상 테스트 환경

Cisco에서는 다음과 같은 가상 머신 환경을 사용하여 일부 AnyConnect 클라이언트 테스트를 수행합니다.

- VMWare ESXi Hypervisor(vSphere) 4.0.1 이상
- VMWare Fusion 2.x, 3.x, 4.x

Cisco에서는 가상 환경에서 실행되는 AnyConnect를 지원하지 않습니다. 그러나 Cisco에서 테스트한 VMWare 환경에서는 AnyConnect가 정상적으로 작동해야 합니다.

가상 환경에서 AnyConnect에 문제가 발생할 경우, 해당 문제를 보고해 주십시오. 최선을 다해 문제를 해결하겠습니다.

AnyConnect 비밀번호에 UTF-8 문자 지원

AnyConnect 3.0 이상 버전을 ASA 8.4(1) 이상 버전과 함께 사용할 경우 RADIUS/MSCHAP 및 LDAP 프로토콜을 사용하여 전송되는 비밀번호에 UTF-8 문자를 지원합니다.

자동 업데이트를 비활성화할 경우 버전 충돌로 인해 연결되지 않을 수 있음

클라이언트가 실행 중인 AnyConnect에서 자동 업데이트를 비활성화할 경우, ASA에 동일한 또는 이하 버전의 AnyConnect가 설치되어 있어야 합니다. 그렇지 않을 경우 클라이언트가 VPN에 연결할 수 없습니다.

이 문제를 방지하려면 ASA에서 동일한 또는 이하 버전의 AnyConnect 패키지를 구성하거나, 자동 업데이트를 활성화하여 클라이언트를 새 버전으로 업그레이드하십시오.

Network Access Manager와 다른 Connection Manager 간의 상호 운용성

Network Access Manager가 작동할 경우, 이 프로그램은 네트워크 어댑터를 단독으로 제어하며 다른 소프트웨어 연결 관리자(Windows 기본 연결 관리자 포함)가 연결을 설정하지 못하도록 차단합니다. 따라서, AnyConnect 사용자가 엔드포인트 컴퓨터에서 다른 연결 관리자(예: iPassConnect Mobility Manager)를 사용하도록 하려면 사용자가 Network Access Manager GUI에서 Disable Client(클라이언트 비활성화) 옵션을 통해 또는 Network Access Manager 서비스를 중단하여 Network Access Manager를 비활성화해야 합니다.

네트워크 인터페이스 카드 드라이버가 Network Access Manager와 호환되지 않음

12.4.4.5 버전의 Intel 무선 네트워크 인터페이스 카드 드라이버는 Network Access Manager와 호환되지 않습니다. 이 드라이버가 Network Access Manager와 동일한 엔드포인트에 설치된 경우, 네트워크 연결이 고르지 않고 Windows 운영 체제가 갑자기 종료될 수 있습니다.

SHA 2 인증서 확인 실패 방지(CSCtn59317)

AnyConnect 클라이언트는 인증서의 Windows 암호화 서비스 공급자(CSP)를 기반으로 IPsec/IKEv2 VPN 연결의 IKEv2 인증 단계 동안 필요한 데이터 해싱 및 서명을 지원합니다. CSP가 SHA 2 알고리즘을 지원하지 않고, ASA에 PRF(Pseudo-Random Function, 의사 난수 함수) SHA256, SHA384 또는 SHA512가 구성되어 있으며, 연결 프로파일(tunnel-group)에 인증서 또는 AAA 인증이 구성되어 있는 경우 인증서 인증이 실패합니다. 사용자에게 인증서 확인 실패 메시지가 전송됩니다.

이러한 실패는 Windows에서만 발생하며, 인증서가 SHA 2 유형 알고리즘을 지원하지 않는 CSP에 속하기 때문입니다. 지원되는 다른 OS에서는 이 문제가 발생하지 않습니다.

ASA의 IKEv2 정책에서 PRF를 md5 또는 sha(SHA 1)로 구성하면 이 문제를 방지할 수 있습니다. 또는 인증서 CSP 값을 사용 가능한 기본 CSP(예: Microsoft Enhanced RSA 및 AES Cryptographic Provider)로 수정할 수 있습니다. 스마트카드 인증서에는 이 해결책을 적용하지 마십시오. CSP 이름은 변경할 수 없습니다. 대신, 스마트카드 공급자에게 문의하여 SHA 2 알고리즘을 지원하는 업데이트된 CSP를 요청하십시오.

⚠ 주의 다음 해결책을 올바르게 수행하지 않을 경우 사용자 인증서가 손상될 수 있습니다. 인증서에 변경 사항을 지정할 경우 각별히 주의하십시오.

Microsoft Certutil.exe 유틸리티를 사용하여 인증서 CSP 값을 변경할 수 있습니다. Certutil은 Windows CA 관리를 위한 명령행 유틸리티이며 Microsoft Windows Server 2003 관리 툴 팩에서 제공됩니다. 다음 URL에서 툴 팩을 다운로드할 수 있습니다.

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

아래 절차에 따라 Certutil.exe를 실행하고 인증서 CSP 값을 변경합니다.

1. 엔드포인트 컴퓨터에서 명령 창을 엽니다.
2. certutil -store -user My 명령을 사용하여 사용자 저장소의 인증서를 현재 CSP 값과 함께 봅니다.

   다음 예시에서는 이 명령에 따라 표시되는 인증서 콘텐츠를 보여 줍니다.

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

3. 인증서에서 <CN> 특성을 식별합니다. 이 예시에서 CN은 Carol Smith입니다. 다음 단계를 진행하려면 이 정보가 필요합니다.

4 다음 명령을 사용하여 인증서 CSP를 수정합니다. 아래 예시에서는 제목 <CN> 값을 사용하여 수정할 인증서를 선택합니다. 다른 특성을 사용할 수도 있습니다.

   Windows 7 이상에서는 certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore -user My <CN> carol smith 명령을 사용합니다.

5 2단계를 반복하고 인증서에 새 CSP 값이 표시되는지 확인합니다.

Host Scan을 위한 안티바이러스 애플리케이션 구성

안티바이러스 애플리케이션은 Posture 모듈 및 Host Scan 패키지에 포함된 애플리케이션의 동작을 악의적인 것으로 잘못 탐지할 수 있습니다. Posture 모듈 또는 Host Scan 패키지를 설치하기 전에 안티바이러스 소프트웨어를 "white-list"에 구성하거나 다음과 같은 Host Scan 애플리케이션에 대한 보안 예외를 설정합니다.

- cscan.exe
- ciscod.exe
- cstub.exe

Microsoft Internet Explorer 프록시가 IKEv2에서 지원되지 않음

IKEv2는 퍼블릭 측 Microsoft Internet Explorer 프록시를 지원하지 않습니다. 이러한 기능에 대한 지원이 필요한 경우 SSL를 사용하십시오. 보안 게이트웨이에서 전송된 컨피그레이션에 따라 지시된 대로, IKEv2 및 SSL은 프라이빗 측 프록시를 지원합니다. IKEv2는 게이트웨이에서 전송된 프록시 컨피그레이션을 적용하며, 후속 HTTP 트래픽은 해당 프록시 컨피그레이션에 따라 달라집니다.

IKEv2에는 그룹 정책의 MTU 조정이 필요할 수 있음

일부 웹 트래픽이 통과하지 못해 일부 라우터의 패킷 조각이 AnyConnect에 수신되고 삭제되는 경우가 간혹 발생합니다.

이 문제를 방지하려면 MTU 값을 낮춥니다. 권장 값은 1200입니다. 다음 예에서는 CLI를 사용하여 이를 조정하는 방법을 보여 줍니다.

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

ASDM을 사용하여 MTU를 설정하려면 **Configuration**(컨피그레이션) > **Network (Client) Access**(네트워크 (클라이언트) 액세스) > **Group Policies**(그룹 정책) > **Add**(추가) 또는 **Edit**(수정) > **Advanced**(고급) > **SSL VPN Client**(**SSL VPN** 클라이언트)로 이동합니다.

DTLS를 사용할 경우 MTU가 자동으로 조정됨

DTLS에 DPD(Dead Peer Detection)가 활성화된 경우, 클라이언트는 경로 MTU를 자동으로 결정합니다. 이전에 ASA를 사용하여 MTU를 줄인 경우, 설정을 기본값(1406)으로 복원해야 합니다. 터널을 설

정하는 동안, 클라이언트는 특수 DPD 패킷을 사용하여 MTU를 자동 조정합니다. 여전히 문제가 발생할 경우, ASA에서 MTU 컨피그레이션을 사용하여 이전과 같이 MTU를 제한하십시오.

Network Access Manager 및 그룹 정책

Windows Active Directory 무선 그룹 정책은 특정 Active Directory 도메인의 PC에 구축된 무선 설정 및 모든 무선 네트워크를 관리합니다. Network Access Manager를 설치할 경우, 관리자는 특정 무선 GPO(Group Policy Object, 그룹 정책 개체)가 Network Access Manager의 동작에 영향을 미칠 수 있다는 점을 숙지해야 합니다. 관리자는 전체 GPO를 구축하기 전에 Network Access Manager로 GPO 정책 설정을 테스트해야 합니다. 다음과 같은 GPO 조건에서는 Network Access Manager가 정상적으로 작동하지 않을 수 있습니다.

- Windows 7 이상에서 **Only use Group Policy profiles for allowed networks(**허용된 네트워크에 연결하는 데 그룹 정책 프로파일만 사용**)** 옵션을 사용 중인 경우

Network Access Manager로 작동 가능한 **FreeRADIUS** 컨피그레이션

Network Access Manager를 사용하려면 FreeRADIUS 컨피그레이션을 조정해야 할 수 있습니다. 취약점을 방지하기 위해 ECDH 관련 암호는 기본적으로 비활성화되어 있습니다. /etc/raddb/eap.conf에서 cipher_list 값을 변경합니다.

액세스 포인트 간에 로밍할 경우 전체 인증 필요

Windows 7 이상을 실행 중인 모바일 엔드포인트에서는 동일한 네트워크에서 액세스 포인트 간에 클라이언트 로밍할 경우 빠른 PMKID 재연결을 활용하는 대신 전체 EAP 인증을 수행해야 합니다. 따라서 활성 프로파일에 모든 전체 인증에 대한 자격 증명을 입력해야 할 경우, AnyConnect에는 해당 작업을 수행하라는 메시지가 표시되기도 합니다.

IPv6 웹 트래픽을 통한 **Cisco Cloud Web Security** 동작에 대한 사용 설명서

IPv6 주소, 도메인 이름, 주소 범위 또는 와일드카드에 대한 예외가 지정되지 않는 한, IPv6 웹 트래픽은 DNS 조회를 수행하는 스캐닝 프록시로 전송되어 사용자가 연결을 시도하고 있는 URL의 IPv4 주소가 존재하는지 확인합니다. 스캐닝 프록시가 IPv4 주소를 찾으면 연결을 위해 이를 사용합니다. IPv4 주소가 없을 경우 해당 연결은 손실됩니다.

모든 IPv6 트래픽이 스캐닝 프록시를 우회하게 하려면, 모든 IPv6 트래픽에 정적 예외 /0을(를) 추가하면 됩니다. 이렇게 하면 모든 IPv6 트래픽이 모든 스캐닝 프록시를 우회합니다. 이는 Cisco Cloud Web Security에서 IPv6 트래픽이 보호되지 않음을 의미합니다.

LAN에서 다른 디바이스의 호스트 이름 표시 차단

AnyConnect를 사용하여 원격 LAN에서 Windows 7 이상 버전에 대한 VPN 세션을 설정하면, 사용자의 LAN에 있는 다른 디바이스의 네트워크 브라우저에 보호되는 원격 네트워크의 호스트 이름이 표시됩니다. 그러나 다른 디바이스는 이러한 호스트에 액세스할 수 없습니다.

AnyConnect 호스트를 통해 서브넷 간에 호스트 이름(AnyConnect 엔드포인트 호스트의 이름 포함)이 유출되지 않도록 하려면 엔드포인트를 마스터 또는 백업 브라우저로 설정하지 마십시오.

1. Search Programs(프로그램 검색) 및 Files(파일) 텍스트 상자에 **regedit**를 입력합니다.
2. **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**로 이동합니다.
3. **MaintainServerList**를 두 번 클릭합니다.

Edit String(문자열 편집) 창이 열립니다.

1. **No(**아니요**)**를 입력합니다.
2. **OK(**확인**)**를 클릭합니다.
3. Registry Editor(레지스트리 편집기) 창을 닫습니다.

해지 메시지

배포 지점이 내부에서만 액세스 가능한 경우 AnyConnect가 LDAP CRL의 배포 지점을 지정하는 서버 인증서를 확인하려고 시도하면 인증 후 AnyConnect 인증서 해지 경고 팝업 창이 열립니다.

이 팝업 창을 표시하지 않으려면 다음 작업 중 하나를 수행합니다.

- 개인 CRL 요건이 없는 인증서를 가져옵니다.
- Internet Explorer에서 선택한 서버 인증서 해지를 비활성화합니다.

주의 Internet Explorer에서 선택한 서버 인증서 해제를 비활성화하면 OS의 다른 기능 사용 시 심각한 보안 영향을 미칠 수 있습니다.

현지화 파일의 메시지가 한 줄 이상의 공간을 차지할 수 있을 경우

현지화 파일에서 메시지를 검색하려는 경우, 아래 예시에 보이는 것처럼 한 줄 이상의 공간을 차지할 수 있습니다.

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

특정 라우터를 활용할 때 **Mac OS X**용 **AnyConnect**의 성능

Mac OS X용 AnyConnect 클라이언트가 IOS를 실행하는 게이트웨이에 대한 SSL 연결을 만들려고 시도하거나 AnyConnect 클라이언트가 특정 유형의 라우터(예: CVO(Cisco Virtual Office) 라우터)를 활용할 때 ASA에 대한 IPSec 연결을 만들려고 시도할 경우, 일부 웹 트래픽은 연결을 통과하지만 다른 트래픽은 삭제될 수 있습니다. AnyConnect가 MTU를 잘못 계산할 수 있습니다.

이 문제를 해결하려면, Mac OS X 명령줄에서 다음 명령을 사용하여 수동으로 AnyConnect 어댑터에 대한 MTU를 더 낮은 값으로 설정합니다.

sudo ifconfig utun0 mtu 1200(Mac OS X v10.7 이상)

Windows 사용자의 상시 연결 우회 방지

Windows 컴퓨터에서 제한된 권한 또는 표준 권한이 있는 사용자는 종종 프로그램 데이터 폴더에 대한 쓰기 액세스 권한을 가질 수 있습니다. 사용자는 이 액세스 권한을 사용하여 AnyConnect 프로파일 파일을 삭제하여 상시 연결 기능을 우회할 수 있습니다. 이를 방지하려면 `C:\ProgramData` 폴더 또는 최소한 Cisco 하위 폴더에 대한 액세스를 제한하도록 컴퓨터를 구성합니다.

무선 호스팅 네트워크 사용 안 함

Windows 7 이상을 사용할 경우 무선 호스팅 네트워크 기능으로 인해 AnyConnect가 불안정해질 수 있습니다. AnyConnect를 사용할 경우, 이 기능을 활성화하거나 이를 활성화하는 프론트엔드 애플리케이션(예: Connectify 또는 가상 라우터)을 실행하지 않는 것이 좋습니다.

AnyConnect를 사용하려면 TLSv1 트래픽을 수락하도록 ASA를 구성해야 함

AnyConnect의 경우 ASA가 SSLv3 트래픽이 아닌 TLSv1 트래픽을 허용해야 합니다. SSLv3 키 파생 알고리즘은 키 파생을 약화시킬 수 있는 방식으로 MD5 및 SHA-1을 사용합니다. SSLv3의 후속 버전인 TLSv1은 이 문제 및 SSLv3에서 나타나는 기타 보안 문제를 해결합니다.

따라서, AnyConnect 클라이언트는 "ssl server-version"의 다음 ASA 설정에 대한 연결을 만들 수 없습니다.

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro가 설치와 충돌

디바이스에 Trend Micro가 있는 경우 드라이버 충돌로 인해 Network Access Manager가 설치되지 않습니다. Trend Micro를 제거하거나 **trend micro common firewall** 드라이버를 선택 취소하여 문제를 방지할 수 있습니다.

Host Scan에서 보고하는 항목

지원되는 안티바이러스, 안티스파이웨어, 방화벽 제품에서는 마지막 스캔 시간 정보를 보고하지 않습니다. Host Scan에서는 다음 내용을 보고합니다.

- 안티바이러스 및 안티스파이웨어의 경우
  - 제품 설명
  - 제품 버전
  - 파일 시스템 보호 상태(활성 스캔)

- 데이터 파일 시간(마지막 업데이트 및 타임스탬프)

- 방화벽의 경우
  - 제품 설명
  - 제품 버전
  - 방화벽 활성화 여부

재연결 지연(CSCtx35606)

IPv6가 활성화되어 있고 Internet Explorer에서 프록시 설정의 자동 검색이 활성화되어 있거나 현재 네트워크 환경에서 지원되지 않을 경우, Windows에 재연결하는 시간이 지연될 수 있습니다. 이를 해결하려면 VPN 연결에 사용되지 않는 모든 물리적 네트워크 어댑터의 연결을 끊거나, 현재 네트워크 환경에서 프록시 자동 검색이 지원되지 않을 경우 IE의 프록시 자동 검색을 비활성화합니다. 릴리스 3.1.03103의 경우, 멀티홈 시스템이 있는 경우에도 재연결 지연이 발생할 수 있습니다.

제한된 권한을 가진 사용자는 ActiveX를 업그레이드할 수 없음

Windows 7 이상 버전에서 제한된 권한을 가진 사용자 어카운트는 ActiveX 컨트롤을 업그레이드할 수 없으므로 웹 구축 방법으로 AnyConnect 클라이언트를 업그레이드할 수 없습니다. 가장 안전한 옵션을 구현하려면 사용자가 헤드엔드에 연결 및 업그레이드하여 애플리케이션 내에서 클라이언트를 업그레이드하는 것이 좋습니다.

참고 이전에 관리자 어카운트를 사용하여 ActiveX 컨트롤을 설치한 경우, 사용자는 ActiveX 컨트롤을 업그레이드할 수 있습니다.

Java 설치 프로그램이 실패할 경우 Mac OS X에서 수동 설치 옵션 사용

사용자가 ASA 헤드엔드의 WebLaunch로 Mac에서 AnyConnect를 시작했을 때 Java 설치 프로그램이 실패하면 대화 상자에 **Manual Install(**수동 설치**)** 링크가 표시됩니다. 이 경우 사용자는 다음 작업을 수행해야 합니다.

1. **Manual Install(**수동 설치**)**을 클릭합니다. 대화 상자에 OS X 설치 프로그램이 포함된 `.dmg` 파일을 저장할 수 있는 옵션이 표시됩니다.
2. 디스크 이미지(`.dmg`) 파일을 열고 Finder를 사용하여 마운트된 볼륨을 찾아 해당 파일을 마운트합니다.
3. 터미널 창을 열고 CD 명령을 사용하여 저장된 파일이 포함된 디렉터리로 이동합니다. `.dmg` 파일을 열고 설치 프로그램을 실행합니다.
4. 설치에 따라 **Applications(**애플리케이션**)** > **Cisco** > **Cisco AnyConnect Secure Mobility Client**를 선택하여 AnyConnect 세션을 시작하거나 Launchpad를 사용합니다.

사전 키 캐싱(PKC) 또는 CCKM 지원 안 함

Network Access Manager는 PKC 또는 CCKM 캐싱을 지원하지 않습니다. Windows 7에서는 Cisco 이외의 무선 카드로 빠른 로밍을 사용할 수 없습니다.

AnyConnect Secure Mobility Client용 애플리케이션 프로그래밍 인터페이스

AnyConnect Secure Mobility Client에는 고유한 클라이언트 프로그램을 작성하려는 사용자를 위한 API(Application Programming Interface)가 포함되어 있습니다.

API 패키지에는 Cisco AnyConnect VPN 클라이언트용 C++ 인터페이스를 지원하는 문서, 소스 파일, 라이브러리 파일이 포함됩니다. Windows, Linux, MAC 플랫폼에서 구축하기 위한 라이브러리 및 예시 프로그램을 사용할 수 있습니다. Windows 플랫폼용 Makefile(또는 프로젝트 파일)도 포함됩니다. 다른 플랫폼에 사용할 수 있도록 예시 코드를 컴파일하는 방법을 보여 주는 플랫폼별 스크립트가 포함되어 있습니다. 네트워크 관리자는 이러한 파일 및 라이브러리를 통해 해당 애플리케이션(GUI, CLI 또는 임베디드 애플리케이션)을 연결할 수 있습니다.

Cisco.com에서 API를 다운로드할 수 있습니다.

AnyConnect API와 관련된 지원 문제의 경우 anyconnect-api-support@cisco.com으로 이메일을 보내 주십시오.

AnyConnect 4.4.03034

해결됨

경고는 Cisco 소프트웨어 릴리스의 예기치 않은 동작 또는 결함을 설명합니다.

The Cisco Bug Search Tool에서 이번 릴리스의 미해결 경고 및 해결된 경고에 대한 자세한 내용을 볼 수 있습니다. Bug Search Tool에 액세스하려면 Cisco 어카운트가 있어야 합니다. 어카운트가 없을 경우 https://tools.cisco.com/RPF/register/register.do에서 등록하십시오.

식별자	구성 요소	제목
CSCvd67481	download-install	클라이언트 컴퓨터에 자동 업데이트를 false로 설정한 AnyConnect 프로파일이 있을 경우 AnyConnect WebLaunch가 실패함
CSCvd90969	fireamp	유효성 검사 코드 서명으로 인해 Windows에서 Fireamp 컨넥터 설치가 실패함
CSCvd85911	gui	OS X 통계 목록 컨트롤을 수정할 수 있음
CSCvc81027	nam	로그온 대화 상자에서 비밀번호 변경 시 언어가 표시되지 않음
CSCvd62921	nam	컴퓨터가 인증된 경우 AnyConnect NAM에서 사용자에게 EAPoL 시작을 1개만 전송함
CSCvd07027	posture-ise	ISE Posture용 서비스 제어 플러그인이 필요함

식별자	구성 요소	제목
CSCvd30861	posture-ise	AnyConnect 4.2에서 connectiondata.xml 파일을 만들 수 없음
CSCvd33055	posture-ise	NAC Agent가 실행 중인 변형을 제거하는 동시에 AnyConnect ISE Posture를 제거함
CSCva01667	vpn	Hyper-V에서 RemoteFX가 사용된 경우 AnyConnect 클라이언트를 연결할 수 없음
CSCvc39267	vpn	재연결하기 전에 AnyConnect 클러스터가 DNS 확인을 위해 재연결함
CSCvc45845	vpn	AnyConnect IKEv2 클러스터 재연결이 전체 터널에서 실행되지 않음
CSCvd53794	vpn	사용자가 원본 네트워크에서 나가고 신뢰할 수 있는 네트워크로 이동할 경우, 원본 네트워크에 대한 IPv6 경로가 보류됨
CSCvd99796	vpn	Mac OS: AnyConnect 터널이 설정된 Touchbar-Macs에 대한 1password 애플리케이션이 중단됨
CSCve12589	vpn	Linux: 다중 로그인한 사용자를 잘못 탐지하여 AC가 연결을 거부함 - Ubuntu 16, RHEL7
CSCve30112	vpn	10.12 이하의 Mac OS에서 스플릿 터널링 중단됨(이중 스택 클라이언트에만 해당)
CSCve39400	vpn	Mac OS - NAT64 단편화로 인해 AnyConnect VPN에 대한 무한 재연결 루프가 발생할 수 있음
CSCvc33765	web security	Websec 클라이언트로 인해 IE11의 성능 문제가 발생함
CSCvd88113	web security	Web Security 모듈로 인해 과도한 GP 업데이트가 발생함
CSCve20800	web security	AnyConnect 4.3 - 시스템이 최대 절전 모드로 전환되지 못함

Open

이 릴리스의 미해결 결함에 대한 최신 정보를 찾아보려면 Cisco Bug Search Tool을 참조하십시오.

AnyConnect 4.4.02039

해결됨

경고는 Cisco 소프트웨어 릴리스의 예기치 않은 동작 또는 결함을 설명합니다.

The Cisco Bug Search Tool에서 이번 릴리스의 미해결 경고 및 해결된 경고에 대한 자세한 내용을 볼 수 있습니다. Bug Search Tool에 액세스하려면 Cisco 어카운트가 있어야 합니다. 어카운트가 없을 경우 https://tools.cisco.com/RPF/register/register.do에서 등록하십시오.

식별자	구성 요소	제목
CSCvd90969	fireamp	유효성 검사 코드 서명으로 인해 Windows에서 Fireamp 컨넥터 설치가 실패함
CSCvd99796	vpn	Mac OS: AnyConnect 터널이 설정된 TouchBar-Macs에 대한 1password 애플리케이션이 중단됨

Open

이 릴리스의 미해결 결함에 대한 최신 정보를 찾아보려면 Cisco Bug Search Tool을 참조하십시오.

AnyConnect 4.4.02034

해결됨

경고는 Cisco 소프트웨어 릴리스의 예기치 않은 동작 또는 결함을 설명합니다.

The Cisco Bug Search Tool에서 이번 릴리스의 미해결 경고 및 해결된 경고에 대한 자세한 내용을 볼 수 있습니다. Bug Search Tool에 액세스하려면 Cisco 어카운트가 있어야 합니다. 어카운트가 없을 경우 https://tools.cisco.com/RPF/register/register.do에서 등록하십시오.

식별자	구성 요소	제목
CSCvd10396	download_install	일부 컴퓨터의 경우 4.1에서 4.4로 업그레이드 도중 AnyConnect가 충돌함
CSCux42801	gui	Enter 키를 눌러 재연결할 경우 AnyConnect가 Advanced Screen(고급 화면)을 실행함
CSCvd23056	gui	크기 조정을 활성화한 경우 AnyConnect 타일 창이 고해상도에서 올바르게 렌더링되지 않음
CSCux95776	nam	NAM으로 최초 win logon 시 잘못된 자격 증명을 사용할 경우 n/w 액세스 불가
CSCvb875955	nam	AnyConnect NAM에 SSID가 표시되지 않을 때가 있음

식별자	구성 요소	제목
CSCvd06041	nam	잠금 후 Windows Surface Pro에서 AnyConnect 연결이 끊김
CSCvd28999	nam	Windows 10을 최소 절전 상태에서 다시 시작할 경우 NAM WiFi 연결이 설정되지 않을 때가 있음
CSCvd510910	nam	사용자 인증이 실패할 경우 NAM이 로그오프 이상으로 확장된 사용자 인증 모드로 전환함
CSCvd51118	posture-asa	Windows 10을 최소 절전 상태에서 다시 시작할 경우 NAM WiFi 연결이 설정되지 않을 때가 있음 Cscan 충돌 - HostScan v4.3.05019
CSCvc99583	posture-ise	특정 시나리오의 경우 Mac 10.12에서 ISE가 탐지되지 않음
CSCvd24513	vpn	클라이언트 방화벽: Windows에서 현재 현지화 기반 동작이 안정적이지 않음
CSCvd33217	vpn	DNS 서버가 없어 재연결 루프가 실패할 경우 캐시된 SG IP가 지워짐
CSCvd53608	vpn	slowDNS 확인 시 VPN 에이전트의 응답을 기다리는 다운로더의 업데이트 시간이 초과함
CSCvd73624	vpn	MacOS: 데스크톱 로그온 시 독립형 Umbrella 모듈(VPN 비활성화됨)이 AnyConnect UI를 시작하지 않음

Open

식별자	구성 요소	제목
CSCvd90969	fireamp	유효성 검사 코드 서명으로 인해 Windows에서 Fireamp 컨넥터 설치가 실패함

이 릴리스의 미해결 결함에 대한 최신 정보를 찾아보려면 Cisco Bug Search Tool을 참조하십시오.

AnyConnect 4.4.01054

해결됨

경고는 Cisco 소프트웨어 릴리스의 예기치 않은 동작 또는 결함을 설명합니다.

The Cisco Bug Search Tool에서 이번 릴리스의 미해결 경고 및 해결된 경고에 대한 자세한 내용을 볼 수 있습니다. Bug Search Tool에 액세스하려면 Cisco 어카운트가 있어야 합니다. 어카운트가 없을 경우 https://tools.cisco.com/RPF/register/register.do에서 등록하십시오.

식별자	구성 요소	제목
CSCvc87398	api	콜백 VpnStateNotification 수신에 문제가 발생함
CSCva28598	core	AnyConnect + Verizon Jetpack(Netgear)으로 인해 Windows 10에 BSOD가 발생함
CSCvc09700	core	Windows 10 버전 1511로 업그레이드 후 영구 경로가 추가됨 - AnyConnect 중단
CSCvc54120	core	AnyConnect 4.3을 통해 RDP 사용자가 LocalUsersOnly 설정에 관계없이 연결할 수 있음
CSCvc12767	download_install	ISE 클라이언트 프로비저닝 하에서 NAC Agent를 제거할 경우 Mac용 NAC가 제거되지 않음
CSCvc43976	gui	Windows SBL 권한 에스컬레이션 취약점에 대한 Cisco AnyConnect Secure Mobility Client
CSCvc73780	gui	4.4.01022: 은폐 모드에서는 기본 설정 창을 표시할 수 없음
CSCvd02715	gui	4.4.0.1048: 클라이언트가 은폐 모드에서 표준 모드로 변경될 경우 시스템 검사 UI가 올바르지 않음
CSCuz57473	nam	SSO를 사용하는 새 사용자에 대해 오류 메시지가 표시되며 NAM이 일정하지 않음
CSCvc56754	nam	NAM 설치 프로그램이 더 이상 DIFxAPI DLL을 제공할 수 없음
CSCvc86615	nam	NAM 관련 UI를 열면 AnyConnect UI 충돌 발생
CSCvc62819	opswat-asa	DAP가 hostscan_4.3.05017로 활성화된 경우 Windows 7 AnyConnect 사용자가 연결할 수 없음
CSCvb99491	opswat-ise	ISE용 Mac 10.12의 Filevault 10.12.x 지원 요청
CSCvc16571	opswat-ise	ISE Compliance 모듈이 Symantec Endpoint Protection 14.x를 지원하지 않음
CSCvc56097	opswat-ise	AVC가 Windows에서 애플리케이션 데이터를 표시할 수 없음
CSCvb49663	posture-ise	필수 요건 상태와 관계없는 선택적인 요건에 대한 치료 팝업 창이 표시됨

식별자	구성 요소	제목
CSCvc14638	posture-ise	네트워크 드라이브에 액세스할 경우 "IT policy prohibits the use of USB storage devices(IT 정책으로 인해 USB 스토리지 디바이스를 사용할 수 없습니다)"라는 메시지가 표시됨
CSCvc47785	posture-ise	Posture 모듈이 OS X 10.9에서 실패함
CSCvc62236	posture-ise	ZipException으로 인해 ISE 2.1 AnyConnectComplianceModuleOSX 3.6.10910.2가 다운로드되지 않음
CSCux13191	vpn	hal-get-property가 없을 경우 CLI가 연결할 수 없음
CSCvb63859	vpn	Linux용 Cisco AC가 메모리에 민감한 정보를 남겨둠
CSCvc00828	vpn	AnyConnect 백업 서버 연결이 프록시를 우회함
CSCvc89318	vpn	AnyConnect 4.3이 RDP 로그온과 로컬 로그온을 구분하지 못하며, AllowRemoteUsers가 작동하지 않음
CSCvc67700	web security	서비스 시작 도중 Web Security 에이전트가 충돌함

Open

이 릴리스의 미해결 결함에 대한 최신 정보를 찾아보려면 Cisco Bug Search Tool을 참조하십시오.

AnyConnect 4.4.00243

해결됨

경고는 Cisco 소프트웨어 릴리스의 예기치 않은 동작 또는 결함을 설명합니다.

The Cisco Bug Search Tool에서 이번 릴리스의 미해결 경고 및 해결된 경고에 대한 자세한 내용을 볼 수 있습니다. Bug Search Tool에 액세스하려면 Cisco 어카운트가 있어야 합니다. 어카운트가 없을 경우 https://tools.cisco.com/RPF/register/register.do에서 등록하십시오.

식별자	구성 요소	제목
CSCuz92464	download_install	Cisco AnyConnect 로컬 권한 에스컬레이션 취약점
CSCvc12767	download_install	ISE 클라이언트 프로비저닝 하에서 NAC Agent를 제거할 경우 Mac용 NAC가 제거되지 않음
CSCuw79769	posture-asa	HostScan이 ASA 헤드엔드에 설정된 로깅 수준을 무시함
CSCva40592	posture-asa	Mac에서 Java 8 사용 시 HostScan/CSD가 ASDM을 정지시킴

식별자	구성 요소	제목
CSCuz55943	posture-ise	PRA 타이머가 꺼지면 AnyConnect 4.x 에이전트에서 PRA 업데이트를 전송하지 않음
CSCva03590	posture-ise	AnyConnect Posture 모듈의 일시적인 충돌
CSCuv65460	vpn	Mac OS X에서 자동 재연결 후 시스템 프록시 설정이 제거됨
CSCva35797	vpn	CVE-2016-2177, CVE-2016-2178용 AnyConnect 평가
CSCvb41365	vpn	Windows 10(1607) 1주년 업데이트 시 프록시를 통한 AnyConnect 연결이 실패함
CSCvb48665	vpn	OpenSSL용 AnyConnect 평가(2016년 9월)
CSCvb62962	vpn	OS X: Deflate 압축이 실행되지 않음(일부 데이터를 전송할 수 없음)
CSCvc04354	vpn	홈 페이지 URL이 AnyConnect 4.3과 작동하지 않음
CSCvc05423	vpn	Mac OS 10.12(Sierra) IPv6 주소 개인정보 기능이 네트워크 불안정을 일으킴

Open

이 릴리스의 미해결 결함에 대한 최신 정보를 찾아보려면 Cisco Bug Search Tool을 참조하십시오.

관련 문서

기타 **AnyConnect** 문서

- Cisco AnyConnect Secure Mobility Client, 릴리스 4.4 릴리스 노트
- Cisco AnyConnect Secure Mobility Client, 릴리스 4.4 관리자 설명서
- AnyConnect Secure Mobility Client 기능, 라이선스, OS, 릴리스 4.4
- *AnyConnect Secure Mobility Client,* 릴리스 *4.4*에서 사용된 오픈 소스 소프트웨어
- Cisco 최종 사용자 라이선스 계약, AnyConnect Secure Mobility Client, 릴리스 4.x

ASA 관련 문서

- Cisco ASA Series 릴리스 노트
- Cisco ASA Series 문서 탐색

- Cisco ASA 5500-X Series Next-Generation Firewalls, 환경 설정 가이드
- 지원되는 VPN 플랫폼, Cisco ASA 5500 Series
- Host Scan 지원 차트

ISE 관련 문서

- Cisco Identity Services Engine, 릴리스 노트, 릴리스 2.2
- Cisco Identity Services Engine 관리 설명서, 릴리스 2.2