제품 구매 및 문의

Cisco Webex Meetings의 보안

서론

Cisco Webex® Meetings를 사용하면 서로 멀리 떨어져 있는 전 세계 직원들과 한 공간에서 일하는 것처럼 실시간으로 협업할 수 있습니다. 이미 전 세계의 많은 기업과 기관, 관공서에서 Cisco® Webex Meetings 솔루션을 활용하여 비즈니스 프로세스를 간소화하고, 영업과 마케팅, 교육, 프로젝트 관리 및 지원 팀의 성과를 개선하고 있습니다.

보안은 모든 기업과 기관 운영에 기본이 됩니다. 그만큼 매우 중요한 관심사입니다. 특히 온라인상에서의 협업에는 회의 예약, 참석자 인증, 문서 공유 등 다양한 작업에 적합한 여러 수준의 보안이 지원돼야 합니다. 시스코는 네트워크, 플랫폼, 애플리케이션의 설계, 개발, 구축, 유지 관리에서 보안을 최우선으로 생각합니다.

Cisco Webex Meetings 솔루션은 가장 엄격한 보안이 필요한 상황에서도 안심하고 비즈니스 프로세스에 통합할 수 있습니다. 이 백서에서는 고객의 투자 결정에 큰 영향을 미치는 Cisco Webex Meetings의 보안 대책과 기본 인프라에 대해 자세히 다룹니다.

참고: 'Cisco Webex Meetings'과 'Cisco Webex Meetings 세션'이라는 용어는 모든 Cisco Webex Meetings 온라인 제품에 사용되는 통합 음성 회의, 인터넷 음성 회의 및 화상 회의를 의미합니다. 특별히 명시하지 않는 한, 이 백서에 기술된 보안 기능은 이 백서에서 언급한 모든 Cisco Webex Meetings 애플리케이션에 동일하게 적용됩니다.

백서 내용

이 백서에서는 Cisco Webex 애플리케이션과 관련 서비스의 보안 기능을 설명합니다. 또한 고객이 Cisco Webex Meetings 플랫폼에서 안심하고 협업할 수 있도록 지원하는 도구와 프로세스, 엔지니어링도 소개합니다.

Cisco Webex Meetings 애플리케이션은 다음과 같은 제품으로 구성되어 있습니다.

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support (Cisco Webex Remote Access 포함)
- Cisco Webex Edge
- Cisco Webex Cloud Connected Audio

Contents

Cisco Webex 보안 모델

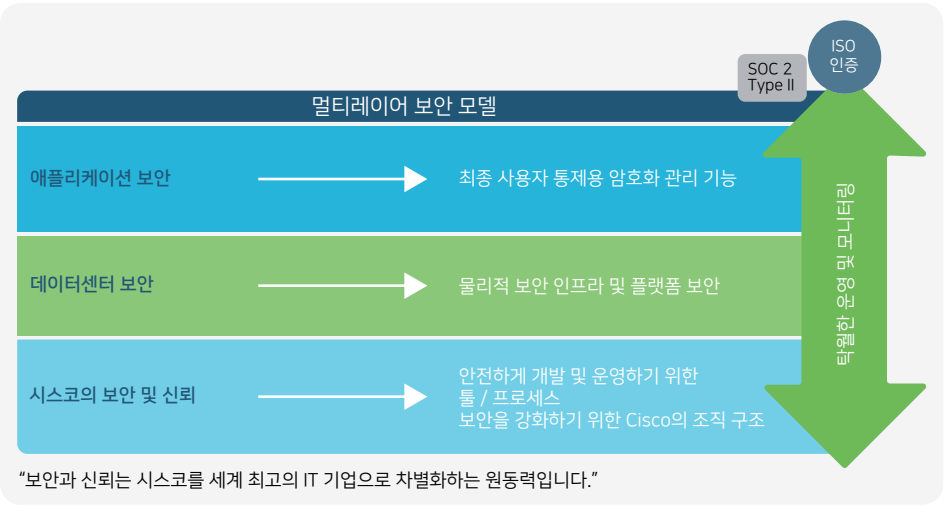
시스코는 클라우드 보안 분야에서 지속적인 리더십을 유지하기 위해 노력하고 있습니다. Cisco STO(Cisco Security & Trust Organization)는 시스코의 모든 팀과 협력하여 핵심 인프라의 설계, 개발, 운영에 활용되는 프레임워크에 보안과 신뢰, 투명성을 더해 모든 부분에서 가장 엄격한 보안 기준을 충족시킵니다.

또한 고객에게 사이버 보안 위험을 줄이고 관리하는 데 필요한 정보를 제공하기 위해 최선을 다하고 있습니다.

Cisco Webex 보안 모델(그림1)은 시스코 프로세스와 동일한 보안 기반에서 구현됩니다.

Cisco Webex 사업부는 기본 원칙을 충실히 따르면서 안전한 Cisco Webex 서비스를 개발, 운영, 모니터링합니다. 이 백서에서는 이러한 원칙도 간추려 설명합니다.

그림1. 시스코 보안 모델



"보안과 신뢰는 시스코를 세계 최고의 IT 기업으로 차별화하는 원동력입니다."

시스코의 보안과 신뢰

시스코 보안 도구 및 프로세스

Cisco SDL(Secure Development Lifecycle)

시스코는 보안을 최우선으로 합니다. 세계 정상급 제품과 서비스를 개발하고 출시하는 시스코는 체계적인 보안 전략을 추구합니다. 시스코의 모든 제품 개발 팀은 Cisco SDL을 따라야 합니다. Cisco SDL은 시스코 제품의 복원력과 신뢰도를 높이도록 설계된 일관적이고 안정적인 프로세스입니다. SDL(Secure Development Lifecycle)의 모든 단계에 도입된 도구와 프로세스, 인식 교육은 심층 방어 체제를 유지하고, 제품의 복원력 대한 전략을 확립하는 데 도움이 됩니다. Cisco Webex 제품 개발 팀은 제품 개발의 모든 단계에서 이 라이프사이클을 철저히 지향합니다.

Cisco SDL(Secure Development Lifecycle)에 대해 자세히 알아보십시오.

시스코의 기본 보안 도구

Cisco STO(Cisco Security & Trust Organization)는 모든 개발자가 일관성을 갖고 보안 조치를 취할 수 있도록 프로세스와 도구를 제공합니다.

이를 통해 제품 개발 프로세스의 불확실성을 해소할 수 있습니다.

시스코의 기본 보안 도구에는 다음이 포함됩니다.

- 제품이 충족해야 하는 제품보안기준(PSB) 요건
- 보안 위협 모델링 과정에 사용되는 위협 툴
- 개발 가이드라인
- 개발자가 자체 제작한 보안 코드가 아닌 기 검증 또는 인증된 라이브러리 사용
- 개발 완료 후 보안 결함을 찾는 데 사용되는(정적 및 동적 분석용) 보안 취약점 테스트
- 시스코 및 타사 라이브러리를 모니터링하고, 취약점이 발견되면 알려주는 소프트웨어 추적

시스코 보안 프로세스 전담 조직

시스코는 보안 프로세스를 전사적으로 구현하고 관리하는 전담 부서를 두고 있습니다. 시스코는 다음과 같은 조직을 기반으로 보안 위협과 문제를 지속적으로 파악합니다.

- Cisco InfoSec Cloud 팀
- Cisco 제품 보안사고 대응 팀(PSIRT)
- 보안 책임 분담

Cisco InfoSec Cloud 팀

클라우드 사업부 최고 보안 책임자가 이끄는 Cisco InfoSec Cloud 팀은 고객에게 안전한 Cisco Webex 환경을 제공할 책임이 있습니다. 이와 같은 목표를 달성하기 위해 Cisco InfoSec Cloud 팀은 Cisco Webex를 고객에게 제공하는 데 관여하는 모든 부서에서 사용할 보안 프로세스와 도구를 규정하고 배포합니다.

그리고 시스코의 다른 팀과 협력하여 Cisco Webex에 대한 모든 보안 위협에 대응합니다. Cisco Webex의 보안 상태 또한 꾸준히 개선하고 있습니다.

Cisco 제품 보안사고 대응 팀(PSIRT)

Cisco 제품 보안사고 대응 팀(Product Security Incident Response Team, 이하 PSIRT)은 시스코 제품 및 서비스와 관련된 보안 문제의 수집, 조사, 보고 업무를 전담하는 글로벌 팀입니다. Cisco PSIRT는 보안 문제의 심각도에 따라 다양한 매체를 사용하여 정보를 게시합니다.

보고 형식은 다음과 같은 조건에 따라 달라집니다.

- 취약점을 해소할 수 있는 소프트웨어 패치 또는 대책을 이미 확보했거나, 심각한 취약점을 해소할 수 있는 코드 픽스를 곧 공개할 예정인 경우
- 시스코 고객에게 더 큰 위험을 줄 수 있는 취약점을 적극적으로 악용한 사례를 Cisco PSIRT가 확인한 경우. 보안 패치가 준비되지 않았더라도, 해당 취약점을 설명하는 보안 공지를 가급적 빨리 게시합니다.
- 시스코 제품에 영향을 미치는 취약점에 대한 대중의 인식 부족으로 시스코 고객이 더 큰 위험에 빠질 수 있는 경우. 이 때도 역시 패치를 배포할 준비가 되지 않았더라도 고객에게 상황을 경고합니다.

어떤 경우든 최종 사용자가 취약점의 영향을 평가하고 자사의 환경 보호에 필요한 조치를 취하기 위해 필요한 최소한의 정보만 공개합니다. Cisco PSIRT는 CVSS(Common Vulnerability Scoring System) 척도를 사용하여 공개된 문제의 심각도를 평가합니다. 아울러 취약점을 악용할 가능성을 고려해 취약점의 세부 정보를 공개하지 않습니다.

Cisco PSIRT에 대한 자세히 내용은 cisco.com/go/psirt에서 확인하실 수 있습니다.

보안 책임

Cisco Webex 그룹의 모든 구성원이 보안에 대한 책임이 있지만, 주요 책임자는 다음과 같습니다.

- 클라우드 사업부 최고 보안 책임자
- 시스코 클라우드 협업 애플리케이션 사업부 부사장 겸 총책임
- 시스코 클라우드 협업 애플리케이션 사업부 엔지니어링 담당 부사장
- 시스코 클라우드 협업 애플리케이션 사업부 제품 관리 담당 부사장

내부 및 외부 침투 테스트

Cisco Webex 그룹은 내부 평가자를 활용해 엄격한 침투 테스트를 정기적으로 실시합니다. 시스코의 엄격한 내부 절차와 별도로 Cisco InfoSec Cloud 팀은 여러 개의 독립평가기관에 시스코의 내부 정책과 절차, 애플리케이션을 엄격히 감사하는 작업을 의뢰합니다. 기업과 정부용 애플리케이션의 미션 크리티컬한 보안 요건을 검증하기 위함입니다. 또한 시스코는 다른 평가 기관과 계약하여 코드 지원 방식의 침투 테스트와 서비스 평가를 지속적이고 심층적으로 실시합니다. 평가 기관은 계약에 따라 다음과 같은 보안 상태를 평가합니다.

- 중요한 애플리케이션/서비스의 취약점 식별 및 솔루션 제시
- 전반적인 아키텍처 개선안 제시
- 코딩 오류 식별, 코딩 작업 개선안 제시

독립평가기관은 Cisco Webex 엔지니어링 직원에게 평가 결과를 직접 설명하고 해결책을 검증합니다. Cisco InfoSec Cloud 팀은 필요한 경우 평가 기관으로부터 증명서를 발급받아 공개할 수 있습니다.

Cisco Webex 데이터센터 보안

Cisco Webex는 Cisco Webex Cloud를 통해 제공되는 SaaS (Software-as-a-Service) 솔루션입니다. Cisco Webex Cloud는 업계 최고의 성능과 통합, 유연성, 확장성, 가용성을 지닌 매우 안전한 서비스 제공 플랫폼입니다. Cisco Webex Cloud는 실시간 온라인 커뮤니케이션용으로 특별히 개발된 솔루션입니다.

Cisco Webex Meetings 세션은 전 세계 여러 데이터센터에 배치된 스위칭 장비를 사용합니다. 데이터센터는 주요 인터넷 액세스 포인트와 가까운 곳에 전략적으로 배치되며, 전용 고대역폭 광섬유 통신을 사용하여 전 세계의 트래픽을 전송합니다. 시스코는 산업 표준 엔터프라이즈급 보안을 기반으로 Cisco Webex Cloud의 전체 인프라를 운영합니다.

또한 시스코는 백본 연결, 인터넷 피어링, 글로벌 사이트 백업 및 캐싱 기술을 지원하는 네트워크 PoP(Point-of-Presence) 센터를 운영하여 최종 사용자에게 제공되는 성능과 가용성을 개선합니다.

물리적 보안

시스코 데이터센터는 시설 및 건물 감시용 CCTV, 출입자 신원 이중 확인 등의 물리적 보안을 갖추고 있습니다. 데이터센터 내에서는 디지털 배지 판독기와 생체 인식 기술을 사용해 접근을 통제합니다. 또한 시스템 다운타임을 방지하기 위해 환경 제어 기술(예: 온도 센서 및 화재 진압 시스템)과 서비스 연속성 유지 인프라(예: 예비 전원)도 구현되어 있습니다.

데이터센터 내부는 인프라의 민감도에 따라 장비에 대한 접근 통제 수준을 달리하는 이른바, '트러스트 존(Trust Zone)'입니다. 예를 들어, 데이터베이스는 안전하게 보관되어 있으며, 네트워크 인프라에는 전용 공간이 따로 있으며, 랙에는 잠금 장치가 설치되어 있습니다. 시스코 보안 인력 외에 신분 확인 절차를 마친 방문객은 시스코 직원이 동행한 경우에만 데이터센터에 들어갈 수 있습니다.

시스코 프로덕션 네트워크에 대한 액세스 역시, 철저히 통제됩니다. 신원이 확인된 소수의 인원만이 네트워크에 액세스할 수 있습니다.

인프라 및 플랫폼 보안

플랫폼 보안은 Cisco Webex Cloud가 관리하는 네트워크, 시스템 및 전체 데이터센터의 보안을 포괄합니다. 모든 시스템은 프로덕션 배포에 앞서 철저한 보안 심사와 승인 검증 과정을 거칠 뿐만 아니라, 배포 후에도 정기적인 강화, 보안 패치, 취약점 검사 및 평가를 받습니다.

서버는 NIST(National Institute of Standards and Technology)가 발행한 STIG(Security Technical Implementation Guidelines)를 사용하여 보강됩니다. 방화벽은 네트워크 경계와 방화벽 자체를 보호합니다. ACL(Access Control List)은 보안 영역을 다양하게 분리합니다. 침입 탐지 시스템(IDS)이 설치되어 활동을 지속적으로 기록하고 모니터링 합니다. Cisco Webex Cloud를 대상으로 매일 내부 및 외부 보안 검사가 실시됩니다. 모든 시스템은 정기 유지 보수의 일환으로 강화 및 패치됩니다. 또한 취약점 검사와 평가가 지속적으로 이뤄집니다.

서비스 연속성 및 재해 복구는 보안 계획의 핵심 요소입니다. 시스코 데이터센터는 글로벌 사이트 백업 체제와 고가용성 설계 구조를 통해 Cisco Webex 서비스의 지리적 장애 조치를 지원 합니다. 단일 장애 지점(SPOF)은 전혀 존재하지 않습니다.

Cisco Webex 애플리케이션 보안

암호화

실행과 동시에 암호화

Cisco Webex 애플리케이션과 Cisco Webex Cloud 간의 모든 통신은 암호화된 채널을 통해 이뤄집니다. Cisco Webex는 TLS 1.2 프로토콜과 고강도 암호화 알고리즘(예: AES 256)만 사용합니다.[1]

TLS를 통해 세션이 구축되면 모든 미디어 스트림(오디오 VoIP, 비디오, 화면 공유 및 문서 공유)이 암호화됩니다.[2]

UDP(User Datagram Protocol)는 미디어 전송에 널리 사용되는 프로토콜입니다. UDP에서 미디어 패킷은 AES 128을 사용하여 암호화됩니다. 초기 키 교환은 TLS 보안 채널에서 이뤄집니다. 또한 각 데이터그램은 인증과 무결성을 위해 해시 기반의 메시지 인증 코드(HMAC)를 사용합니다.
Code (HMAC) for authentication and integrity.

종단간 암호화

클라이언트에서 Cisco Webex 서버로 이동하는 미디어 스트림은 Cisco Webex 방화벽을 통과한 후에 해독됩니다. 이때 시스코가 네트워크 기반의 녹화 방식을 지원하므로 향후에 참조할 목적으로 미디어 스트림을 녹화할 수 있습니다. 그런 다음 Cisco Webex는 다른 클라이언트로 미디어 스트림을 전송하기 전에 다시 암호화합니다. 그러나 더 수준 높은 보안이 필요한 기업을 위해 종단간 암호화 기능도 지원합니다. 이 옵션을 선택하면 Cisco Webex Cloud가 미디어 스트림을 해독하지 않습니다. 종단간 암호화도 일반적인 통신과 마찬가지로 Cisco Webex Cloud는 클라이언트-서버 통신용 TLS 채널을 수립후 동작합니다.

또한 모든 Cisco Webex 클라이언트는 키 페어(Key Pair)를 생성하고 공개 키를 호스트의 클라이언트에게 전송합니다. 호스트는 CSPRNG(Cryptographically Strong Secure Pseudo-Random Number Generator)를 사용하여 임의의 대칭 키를 생성하고, 클라이언트가 전송하는 공개 키를 사용하여 대칭 키를 암호화한 다음, 다시 클라이언트로 전송합니다.

클라이언트에 의해 생성된 트래픽은 대칭 세션 키를 사용하여 암호화됩니다. 이런 모델에서는 Cisco Webex 서버가 트래픽을 해독할 수 없습니다.

종단간 암호화 옵션은 Cisco Webex Meetings와 Cisco Webex Support에서 사용할 수 있습니다. 종단간 암호화 기능을 활성화한 상태에서는 다음과 같은 기능을 사용할 수 없습니다.

- Web 기반 미팅 앱
- 네트워크 기반 녹화
- 주최자보다 먼저 회의실 입장
- 비디오 엔드포인트

다양한 암호화 알고리즘

Cisco Webex는 통신 보안을 위해 다음과 같은 암호화 알고리즘을 지원합니다. 따라서 고객은 자신의 환경에 최적화된 암호화 알고리즘을 선택하여 사용할 수 있습니다. 표1에는 암호화 알고리즘과 각 알고리즘의 비트 길이가 제시되어 있습니다.

[1] 실제 암호화 프로토콜 및 강도는 호스트가 Cisco Webex와 연결하려는 OS 및 브라우저 설정에 따라 다릅니다.

[2] 타사 화상회의 장비를 사용하여 클라우드 회의에 접속하는 사용자가 송수신하는 미디어 스트림은 암호화되지 않을 수 있습니다. 이 경우 방화벽 설정을 통해 Cisco Webex에서 송수신하는 암호화되지 않은 트래픽의 보안을 강화하시길 바랍니다. 그러나 방화벽 밖에 있는 참석자가 타사 화상회의 장비를 사용하여 회의에 참석하는 것을 허용할 경우, 회의 데이터가 암호화되지 않은 채 전송될 수 있습니다.

표 1. 암호화 알고리즘 및 비트 길이

암호화 알고리즘	비트 길이
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	128

유휴 데이터 보호

Cisco Webex Meetings가 비즈니스에 중요한 회의 및 사용자 데이터를 저장하도록 설정할 수 있습니다. Cisco Webex Meetings는 다음과 같은 기능을 통해 유휴 데이터를 보호합니다.

- SHA-2(단방향 해싱 알고리즘) 및 Salt를 사용하여 모든 사용자 비밀번호를 저장합니다.
- 회의용 또는 녹화용 비밀번호도 함께 암호화 합니다.
- 저장된 네트워크 기반의 녹화 데이터를 암호화합니다. Webex 녹화 데이터는 파일 단위와 논리 볼륨 단위로 암호화됩니다. 파일 키는 256비트 블록 AES GCM 키입니다. 이 파일 키는 정책에 따라 순환되는 AES HmacSHA256 기반의 마스터 키로 암호화된 후 데이터베이스에 저장됩니다. 재생 및 다운로드의 경우 작업 이전 또는 도중에 암호화된 녹화 파일이 해독됩니다. 시스코는 고객을 위해 위의 키들을 안전하게 관리합니다.

Cisco Webex 역할 기반 접근제어

Cisco Webex 애플리케이션은 저마다 다른 권한이 부여된 5가지 역할 중 선택하여 액세스할 수 있도록 설계되었습니다. 5가지 역할은 다음과 같습니다.

주최자

주최자는 Cisco Webex 회의를 예약하고 시작합니다. 주최자는 모든 사람의 회의 환경을 통제하고, 회의를 예약할 때와 회의 중에 그와 관련한 결정을 내립니다.

사이트 관리자는 주최자의 통제권을 조정할 수 있습니다. 사이트 관리자가 제한하지 않는 한 주최자는 회의 보안 유지 방법을 선택할 수 있습니다.

대리 주최자

예약하는 동안 주최자는 대리 주최자를 배정할 수 있습니다. 주최자를 대신하여 회의를 시작할 수 있는 대리 주최자는 기본적으로 주최자와 동일한 권한을 가집니다.

주최자는 회의 도중 다른 사용자에게 주최자 권한을 이양할 수 있습니다. 주최자와 대리 주최자의 보안 관련 권한은 동일합니다.

발표자

발표자는 프레젠테이션, 특정 애플리케이션 또는 데스크톱 전체를 공유할 수 있습니다. 발표자는 메모 도구를 제어합니다. 보안 관점에서 발표자는 공유하는 애플리케이션과 데스크톱에 대한 원격 제어 권한을 개별 참석자에게 부여하고 철회할 수 있습니다.

패널(교육 및 이벤트 전용)

패널의 주요 역할은 주최자와 발표자가 이벤트를 원활하게 진행하도록 지원하는 것입니다. 참석자가 패널의 역할을 병행할 수 있습니다. 주최자는 Q&A 세션에서 패널에게 해당 분야 전문가 역할을 맡아 참석자의 질문을 확인하고 답하거나, 공개 및 비공개 채팅 메시지에 응답하거나, 공유 콘텐츠에 메모를 추가하거나, 투표 진행자 역할을 맡아 투표를 진행하도록 요청할 수 있습니다.

참석자

발표자 또는 주최자 역할이 배정되지 않은 한, 참석자는 보안 책임이나 권한을 갖지 않습니다. 사이트 관리자와 주최자는 회의 도중 언제든지 참석자에게 Cisco Webex 회의 주도권(발표자 역할)을 넘길 수 있습니다. 이 설정은 기본적으로 비활성화되어 있습니다.

사이트 관리자

계정 관리뿐만 아니라 정책을 관리하고 사이트 또는 각 사용자에게 정책을 시행할 수 있습니다. 사이트 관리자는 다른 모든 역할 및 사용자가 사용할 수 있는 Cisco Webex 기능을 선택할 수 있습니다.

관리 기능

Cisco Webex는 Cisco Webex 사이트를 비즈니스 요건에 맞게 효과적으로 관리할 수 있는 상세한 사이트 관리 기능을 지원합니다. 모든 보안 기능에 대한 자세한 내용은 Cisco Webex 사이트 관리 가이드를 참조하십시오.

계정 관리

계정 관리 기술을 Cisco Webex와 통합하여 SSO(Single Sign-On)를 구현하고, 계정 관리 및 액세스 정책을 완벽하게 제어할 수 있습니다. Cisco Webex에 계정을 개설한 경우 다수의 사이트 관리 기능을 사용해 필요에 맞게 계정을 관리할 수 있습니다.

- SHA-2 SSL 인증서의 SSO 지원

사이트 관리자는 다음을 수행할 수 있습니다.

- 지정된 횟수만큼 로그인 시도가 실패한 경우 계정 잠금
- 지정된 기간이 지나면 잠긴 계정의 잠금 자동 해제
- 지정된 기간 동안 활동이 없는 경우 계정 비활성화
- 다음에 로그인할 때 사용자에게 비밀번호를 변경하도록 요구
- 사용자 계정 잠금/잠금 해제
- 사용자 계정 활성화/비활성화
- 신규 계정 개설 시 보안 텍스트 입력 요구
- 신규 계정 개설 시 이메일 확인 요구
- 신규 계정 자동 등록(가입) 허용
- 신규 계정 자동 등록 규칙 설정
- 참석자가 한 명인 경우 회의를 자동으로 종료하도록 보안 옵션 설정
- 가능한 경우 전화 접속 사용자의 발신자 번호 표시

관리자는 다음과 같은 옵션을 사용하여 비밀번호 기준을 관리할 수 있습니다.

- 대소문자 혼용
- 최소 길이
- 숫자, 알파벳 또는 특수 문자의 최소 개수
- 3번 이상 한 문자의 반복 사용 불가
- 지정된 횟수 이상 이전 비밀번호 재사용 불가
- 동적 텍스트(사이트 이름, 주최자 이름, 사용자 이름) 사용 불가
- 설정 목록에 있는 문구의 비밀번호 사용 불가(예: 'password')
- 지정된 기간 동안 비밀번호 변경 불가
- 지정된 기간마다 주최자의 계정 비밀번호 변경 요구
- 다음 로그인 시 모든 사용자에게 계정 비밀번호 변경 요구
- '공통 사이트 설정(Common Site Settings) 옵션(Options)'에서 이뤄진 설정 변경을 보여주는 사이트 구성 감사 로그 다운로드
- 예약된 회의용 호스트 키를 사이트에서 검색하려는 경우 인증 요구
- 주최자의 개인 아바타 업로드 기능 비활성화

회의 설정

회의용 세부 설정을 사용하여 회의 이전, 도중, 이후에 사용자 및 시스템의 작업을 관리할 수 있습니다. 대부분의 경우 이런 설정은 Cisco Webex Meetings, Cisco Webex Events, Cisco Webex Training이 모든 사용자에 필요한 용도에 맞춰 저마다 다르게 반응하도록 중앙 집중식으로 적용할 수 있습니다. 또한 세션 유형 설정을 사용하여 각 사용자 그룹의 파일 전송, 데스크톱 공유, 녹화 등 여러 회의용 기능을 활성화 또는 비활성화할 수 있습니다.

지원되는 회의 설정은 다음과 같습니다.

- 향후 손쉬운 회의 주최 및 참석을 위해 사용자의 이름과 이메일 주소 저장 허용
- 주최자가 다른 주최자에게 녹화 권한 이양 허용
- 사이트에 액세스하려는 모든 주최자와 참석자에게 인증 요구
- 원격 액세스 서비스에 강한 비밀번호 규칙 적용
- 목록에 공개된 모든 회의 숨기기
- 모든 회의에 비밀번호 요구
- 비밀번호 초기화 시 관리자의 승인 요구
- 다른 주최자의 대리 회의 예약 허용
- 예약 시 주최자의 대리 주최자 지정 허용
- Dropbox 및 Box와 같은 외부 통합 솔루션과 콘텐츠 공유 (iPad로 발표 시)
- 참석자가 한 명인 경우 지정된 시간이 지나면 회의 자동 종료 (예약된 회의, Webex Personal Rooms 회의 및 음성 전용 회의에 적용)
- 전화 또는 화상 회의 시스템으로 회의에 참석하려는 경우 회의용 비밀번호 요구
- 모든 회의 참석자(주최자 포함)에게 면책 조항 고지
- 녹화 데이터의 열람 및 다운로드 전에 참석자에게 면책 조항 고지
- 주최자보다 먼저 참석자의 회의실 입장 허용
- 주최자보다 먼저 참석자의 전화 회의 참석 허용
- 로그인한 사용자의 녹화 데이터 보기 제한
- 녹화 데이터 다운로드 금지
- 모든 네트워크 기반 녹화에 비밀번호 요구

이러한 설정 대부분을 사이트 관리자가 그대로 두면 전체 사이트에 일반적인 수준의 보안 통제가 적용됩니다. 주최자는 필요에 따라 특정 회의의 보안 수준을 결정할 수 있습니다. 예를 들어, 사이트 관리자는 회의 참석자에게 로그인 프로세스를 요구하지 않도록 설정할 수 있지만, 각 주최자는 회의의 보안 유지를 위해 로그인한 참석자만 해당 회의실에 입장하도록 설정할 수 있습니다.

개인 회의실 보안 설정

모든 Cisco Webex 주최자는 회의에 사용할 수 있는 개인 회의실 전용 URL을 받을 수 있습니다. 개인 회의실 URL은 https://sitename.webex.com/meet/username처럼 구성되어 있습니다. 주최자 또는 Cisco Webex 관리자는 사용자 이름을 변경할 수 있습니다. 개인 회의실을 사용하면 참석자가 회의에 참석하기 위해 이메일이나 일정을 찾을 필요가 없기 때문에 협업이 훨씬 수월해집니다. 개인 회의실은 주최자가 개설할 수 있는 일종의 개인용 가상 회의실입니다.

관리자용 개인 회의실 보안 설정은 다음과 같습니다.

- 주최자의 개인 회의실(Webex Meeting 클라이언트 및 비디오 엔드포인트)에 입장하려는 참석자에게 인증을 요구합니다.
- 참석자가 로비에 대기 중인 경우 주최자에게 이를 알릴 수 있습니다.
- Webex Meeting 클라이언트 및 비디오 엔드포인트를 사용하여 로비에 입장할 수 있습니다.
  (비디오 엔드포인트로 개인 회의실에 입장하는 데 사용되는)
- 주최자 PIN 길이를 설정합니다.
- 주최자가 승인할 때까지 로비와 개인 회의실에 있는 무단 참석자를 차단할 수 있습니다.

주최자용 개인 회의실 보안 설정은 다음과 같습니다.

- 언제든지 개인 회의실을 수동으로 잠글 수 있습니다.
- 지정된 시간이 지나면 개인 회의실이 자동으로 잠기도록 설정할 수 있습니다. 이 설정은 Webex Meetings 클라이언트 및 비디오 엔드포인트로 개설한 개인 회의실에 적용됩니다.
- 잠겨 있는 개인 회의실에 입장하려는 회의 참석자는 로비에 대기하도록 요구하고, 주최자가 수동으로 입장을 허용할 수 있습니다.
- 개인 회의실이 열려 있더라도 참석자가 로비에서 설정된 인증 절차를 마쳐야 하고, 주최자는 수동으로 입장을 허용할 수 있습니다. 허가 받은 직원은 어느 방에나 들어갈 수 있지만, 신원이 확인되지 않은 방문자는 직원의 안내를 받아야 하는 실제 회의실과 유사합니다.
- 부재중일 때 누군가 개인 회의실에 입장한 경우 이메일 알림을 보내도록 설정할 수 있습니다.

SSO(Single Sign-On)

Cisco Webex는 SAML(Security Assertion Markup Language) 2.0 프로토콜을 통해 SSO 통합 인증을 지원합니다.

사이트 관리자는 공개 키 X.509 인증서를 사용자 정의된 Cisco Webex 사이트에 업로드해야 합니다.

그러면 사용자 특성이 포함된 SAML Assertion을 생성하고 일치하는 개인 키로 디지털 서명을 실시할 수 있습니다. Cisco Webex는 사용자를 인증하기 전에 미리 설치된 공개 키 인증서와 대조하여 SAML 서명의 유효성을 검사합니다.

고객의 액세스 관리 또는 ID 솔루션과 Cisco Webex 사이트는 SAML Assertion을 공유합니다. 고객의 솔루션(예: Microsoft Active Directory Federation Services, PingFederate, CA Siteminder Single Sign-On, OpenAM 또는 Oracle Access Manager)은 IdP(Identity Provider) 역할을 합니다. Cisco Webex 사이트는 서비스 제공업체 역할을 하며 Cisco service-provider-initiated 와 IdP-initiated SSO flows 모두 지원합니다.

Cisco Webex에 SSO를 구현하면 회사 정책에 따라 사용자 및 액세스를 완벽하게 관리할 수 있습니다. 장점은 다음과 같습니다.

- IdP는 사용자 자격 증명(인증서, 지문 또는 기타)의 유효성을 검사하는 주체입니다.
- 고객은 SaaS 기반 서비스마다 다른 솔루션을 사용하는 방식 대신, 2단계의 통합 사용자 인증 방식을 구현할 수 있습니다.
- Cisco Webex는 사용자 자격 증명을 저장하지 않습니다.
- 고객이 Cisco Webex에 액세스하는 사람을 통제합니다.
- 사용자가 기업 IdP 가입 또는 탈퇴 프로세스를 쉽게 이해할 수 있습니다.

Cisco Webex 추가 기능 및 보안

비디오 장치로 회의 참석

사용자는 비디오 장치를 사용하여 Cisco Webex 회의에 참석하거나 Cisco Webex 회의를 시작할 수 있습니다. 이를 위해서는 Cisco Webex Meetings 사이트에서 해당 기능을 활성화해야 합니다. 이 기능을 활성화하면 사용자가 Cisco TelePresence® 엔드포인트, 소프트 클라이언트, Skype for Business 클라이언트 또는 타사의 표준 기반 비디오 장치를 사용하여 비디오 주소로 전화를 거는 방식으로 회의에 참석할 수 있습니다. 사용자가 자동 무선 페어링을 통해 장치에서 회의에 참석할 수 있으므로 시스코 엔드포인트의 환상적인 효율성이 보장됩니다.

고객 위치에 별도의 비디오 브리징 장비를 설치하지 않아도 비디오 장치가 정상적으로 작동합니다. 비디오 브리징 기능은 Cisco Webex Meeting Center와 동일한 보안 수준의 Cisco Webex Cloud에 구현되며, 동일한 산업 등급 보안 체제(물리적, 네트워크, 인프라 및 관리)를 사용합니다. 비디오 엔드포인트는 신호 전송용 SIP(Session Initiation Protocol) 및 H.323과 RTP/SRTP(Real-Time Transport Protocol/Secure Real-Time Protocol) 미디어를 통해 회의에 접속할 수 있습니다. Webex Meetings는 SIP용 TLS 전송과 미디어용 SRTP 전송을 지원합니다. 비디오 엔드포인트가 SIP/TLS를 통해 회의에 접속한 경우 미디어 스트림은 SRTP를 통해 암호화됩니다.

H.235는 H.323 회선의 보안 유지에 사용됩니다.

또한 비디오 장치를 사용하여 회의에 참석하려는 경우 비밀번호를 요구하도록 사이트를 설정할 수도 있습니다.

CCA(Cloud Connected Audio)

Cisco Webex CCA는 온프레미스 IP 텔레포니 네트워크를 사용하여 Cisco Webex 회의에 통합 오디오 환경을 지원하는 토털 오디오 솔루션입니다. 텔레포니 회선을 사용하는 기존 방식 대신, 온프레미스의 SIP 트렁크를 Cisco Webex 데이터센터에 연결합니다. 이 솔루션은 다른 모든 Cisco Webex 오디오 옵션과 동일한 수준의 직관적인 통합 사용자 환경을 지원합니다. 특히 Cisco Teleex CCA는 IP 텔레포니 네트워크를 사용하므로 오디오 서비스 비용을 절감할 수 있습니다.

CCA 환경은 완벽하게 캡슐화되어 있습니다. 인터넷에서 CCA에 접근하거나 각종 공격 수법으로도 침투하기가 매우 어렵습니다. 인프라는 공유하지만 테넌트 간에 라우팅이 이뤄지지 않으므로 다른 테넌트의 악성 트래픽이 완벽히 차단됩니다. 또한 트렁크를 통한 트래픽은 필요한 Cisco Webex 인프라 포트에 연결된 라우팅 프로토콜 및 UDP(User Datagram Protocol) 패킷으로 제한됩니다. Cisco Webex 인프라는 사전 구성된 DP(Dial Peer)의 트래픽만 수신하도록 구성되어 있습니다.

CCA는 P2P 비공개 회선을 통해 Cisco Webex 플랫폼에 연결됩니다. CCA 회선의 종착지는 고객 전용 포트입니다.

CCA 회선은 고객의 데이터센터와 시스코의 데이터센터에 구현된 에지 라우터와 방화벽에 대한 액세스 제어 목록으로 보호받습니다.

CCA 서비스는 IP 서브넷을 분할하며, Cisco Webex의 CUBE (Cisco Unified Border Element) IP 세그먼트만 고객에게 공개됩니다. 고객은 다른 고객의 IP나 CUBE를 전혀 알 수 없습니다.

요약하자면 Cisco Webex CCA는 불필요한 트래픽 과부하를 유발하거나 설계를 저해하지 않으면서 강력한 보안을 지원합니다.

Cisco Webex 개인 정보 보호

고객 데이터 보호, 보존 및 규정 준수

Cisco Webex는 고객 데이터 보호에 만전을 기합니다. 시스코는 개인 정보 보호 정책을 준수하면서 고객 정보를 수집, 사용, 처리합니다. 자세한 내용은 Cisco Webex 서비스 약관에서 확인하실 수 있습니다.

Cisco Webex Meetings는 Privacy Shield Framework 인증을 받았습니다.

Cisco Webex는 적용되는 합법적 전송 메커니즘에 따라 관리 데이터, 지원 데이터, 원격 측정 데이터를 EU에서 미국으로 (또는 적절한 경우 다른 허용 국가로) 전송합니다. 이러한 데이터 범주의 정의는 다음과 같습니다.

관리 데이터 : 시스코의 제품 또는 서비스 제공 상태를 관리하거나, 시스코의 자체적인 비즈니스 목적으로 고객 또는 타사의 계정을 관리하기 위해 시스코가 수집하고 사용하는 고객 또는 타사의 직원 또는 대리인에 관한 정보입니다. 관리 데이터에는 이름, 주소, 전화번호, 이메일 주소, 시스코와 타사 간의 계약 조건에 관한 정보가 포함됩니다. 이러한 데이터는 최초 등록 시점에 수집되거나 시스코 제품 관리의 일환으로 나중에 수집되기도 합니다. 제품 관리의 일환으로 나중에 수집되기도 합니다.

또한 관리 데이터에는 고객의 직원 또는 대리인이 Cisco Webex에서 정한 회의 제목, 회의 시간 및 기타 회의 속성도 포함될 수 있습니다. 관리 데이터의 다른 예로는 Cisco Webex 에서 주최한 회의 제목, 회의 시간 및 기타 회의 속성이 있습니다.

고객 데이터 : 고객이 시스코 제품 또는 서비스를 사용하기 위해 시스코에 제공하거나 작업지시서 또는 계약서에 따라 고객으로부터 특별히 요청받아 시스코가 개발한 모든 데이터(예: 텍스트, 음성, 비디오, 이미지 파일, 녹화 데이터)를 포괄합니다. 고객 데이터에는 로그, 구성 또는 펌웨어 파일 및 코어 덤프(core dump)가 포함됩니다. 지원 요청의 일환으로 시스코의 문제 해결을 돕기 위해 제품이나 서비스에서 수집하여 시스코에 제공하는 데이터도 포함됩니다. 그러나 관리 데이터, 지원 데이터, 원격 측정 데이터는 고객 데이터에 해당되지 않습니다.

지원 데이터 : 고객이 하드웨어 또는 소프트웨어에 대한 정보를 포함하여 지원 서비스 또는 기타 문제 해결 요청서를 제출하는 과정에서 시스코에 제공하는 정보입니다. 인증 정보, 소프트웨어 설치 및 하드웨어 구성에 관한 제품, 시스템 및 레지스트리 데이터 상태 정보, 오류 추적 파일 같은 지원 문제와 관련된 세부 정보가 포함됩니다. 로그, 구성 또는 펌웨어 파일, 또는 지원 요청의 일환으로 시스코의 문제 해결을 돕기 위해 제품에서 수집하여 시스코에 제공하는 코어 덤프는 지원 데이터에 해당되지 않습니다. 이런 데이터는 모두 고객 데이터에 해당됩니다

원격 측정 데이터 : 제품 또는 서비스를 사용하고 운영하는 과정에서 계측 및 로깅 시스템이 생성하는 정보입니다.

Cisco Webex Cloud에서 수집된 모든 데이터는 여러 계층의 강력한 보안 기술 및 프로세스로 보호받습니다. 고객 데이터를 보호하기 위해 Cisco Webex 환경의 여러 계층에 배치된 보안 통제 조치는 다음과 같습니다.

- **물리적 액세스 제어** : 생체 인식 기술, 디지털 배지 및 비디오 감시를 통해 물리적 접근이 통제됩니다. 데이터센터에 출입하려면 허가를 받아야 하며, 출입은 전자 발권 시스템을 통해 관리됩니다.
- **네트워크 액세스 제어** : Cisco Webex 네트워크 경계는 방화벽으로 보호받습니다. Cisco Webex 데이터센터에서 송수신하는 모든 네트워크 트래픽은 침입감지시스템(IDS)을 통해 지속적으로 모니터링됩니다. 또한 Cisco Webex 네트워크는 별도의 보안 영역으로 분리됩니다. 보안 영역 간에 송수신되는 트래픽은 방화벽과 ACL(액세스 제어 목록)을 통해 통제됩니다.
- **인프라 모니터링 및 관리 기능** : 네트워크 장치, 애플리케이션 서버, 데이터베이스를 포함한 모든 인프라 구성 요소는 엄격한 지침으로 보강되며, 보안 문제를 식별하고 해결하기 위해 정기적으로 검사를 받습니다.
- **암호화 기능** : Cisco Webex 데이터센터와 Cisco Webex 클라이언트가 주고 받는 모든 데이터는 암호화됩니다. 단, 클라우드 지원 회의에서 암호화되지 않은 비디오 장치는 예외입니다. 또한 Cisco Webex에 저장되는 중요한 데이터 (예: 비밀번호)도 암호화됩니다.

고객이 지원 상의 이유로 액세스를 요청하지 않는 한 시스코 직원은 고객 데이터에 액세스하지 않습니다. 시스코 직원이 시스템에 액세스해야 하는 경우에도 반드시 '업무 분리' 원칙에 따라 관리자의 승인을 받습니다. 알아야 하는 범위 내에서 맡은 작업 수행에 필요한 액세스 권한만 시스코 직원에게 부여됩니다. 또한 정기적인 심사를 통해 시스코 직원이 규정에 따라 시스템에 액세스했는지 확인합니다. 액세스 권한을 가진 직원은 매년 ISO (International Organization for Standardization) 27001 정보 보안 인식 교육을 받아야 합니다.

이와 같은 모든 특수한 통제 외에도 모든 시스코 직원은 신원 확인을 받고, 비밀 유지 계약(NDA)에 서명하며, COBE(Code of Business Ethics) 교육 과정을 이수합니다.

HIPAA
(Health Insurance Portability and Accountability Act)

고객이 요구한 경우 시스코는 Cisco Webex의 기능, 기술, 보안에 관한 정보를 제공합니다. HIPAA가 적용되는 기업은 자사의 법률 고문과 상의하여 Cisco Webex의 기능이 비즈니스 프로세스와 GDPR를 준수하기에 적합한지 확인해야 합니다.

- GDPR 준비도
- Cisco Webex Meetings 개인 정보 보호 시트

산업 표준 및 인증

Cisco Webex는 엄격한 내부 표준을 준수할 뿐만 아니라 정보 보안에 만전을 다하고 있음을 입증하기 위해 지속적으로 인증 기관의 검증을 받습니다. Cisco Webex는 다음과 같은 인증을 완료했습니다.

- ISO 27001 인증
- SOC(Service Organization Controls) 2 Type II 감사
- FedRAMP 인증
  (자세한 내용, 범위, 가용성은 cisco.com/go/fedramp 참조)
  참고: FedRAMP 인증을 받은 Webex 서비스는 미국 정부 및 교육 기관 전용 서비스입니다.
- C5(Cloud Computing Compliance Controls Catalogu) 증명
- 개인 정보 보호 체계(Privacy Shield Framework) 인증

마치며

웹 및 화상 회의 분야에서 업계 최고로 검증받은 Cisco Webex 솔루션을 통한 협업으로 더 많은 일을 더 빠르게 수행해보세요. Cisco Webex는 엄격한 내부 및 산업 표준을 준수하기 위해 지속적으로 관련 기관의 검증과 인증을 받는 확장식 아키텍처, 일관적인 가용성, 다계층 보안을 제공합니다. 시스코는 모든 것을 더 안전하게 연결하여 모든 일을 가능하게 만들어드립니다.

제품 구매 및 문의

문의하기

추가 정보

Cisco Webex 솔루션에 대한 자세한 내용은 다음 사이트를 참조하십시오.

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support
- Cisco Webex Cloud Connected Audio

C11-737588-02 02/19