

Introducción

Permitir la colaboración en tiempo real para conectar a los empleados globales y los equipos virtuales es una tendencia creciente entre organizaciones que buscan una ventaja competitiva. En todo el mundo, una gran cantidad de empresas y agencias gubernamentales confían en las soluciones de Software-as-a-Service (SaaS) de Cisco WebEx™ para agilizar los procesos comerciales de ventas, marketing, formación, gestión de proyectos y soporte. Cisco® hace de la seguridad su mayor prioridad en el diseño, empleo y mantenimiento de su red, plataforma y aplicaciones. Por ello, puede incorporar las soluciones de WebEx® en sus procesos de negocio en curso (de forma instantánea y con confianza), incluso en entornos con las exigencias de seguridad más estrictas.

Comprender las características de seguridad de las aplicaciones en línea de Cisco WebEx y la infraestructura de comunicación subyacente (la Cisco Collaboration Cloud) es un componente importante en su decisión de compra.

Descubra la información detallada de seguridad para:

- La infraestructura Cisco Collaboration Cloud
- La experiencia de reuniones seguras de WebEx
 - Configurar el sitio de la reunión
 - Planificar opciones de seguridad
 - Iniciar y unirse a una reunión de WebEx
 - Tecnologías de cifrado
 - Seguridad de la capa de transporte
 - Compatibilidad de cortafuegos
 - Almacenamiento de datos posterior a la reunión
 - Single Sign On (Inicio de sesión único)
- Acreditaciones a terceras personas: auditorías independientes validan la seguridad de Cisco WebEx

Los términos "reuniones de Cisco WebEx" y "sesiones de reunión de Cisco WebEx" hacen referencia a los servicios de conferencias con audio integrado, teléfono a través de Internet y conferencias de vídeo desde un único punto y desde varios puntos empleados en todos los productos en línea de Cisco WebEx, que incluyen:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center (incluyendo Cisco WebEx Remote Support y Cisco WebEx Remote Access)

Salvo que se especifique lo contrario, las características de seguridad descritas en este documento pertenecen por igual a todas las aplicaciones y servicios de WebEx mencionados arriba.

Roles en las reuniones WebEx

Los cuatro roles clave en una reunión de WebEx son organizador, organizador alternativo, presentador y asistente.

Organizador

El organizador planifica e inicia las reuniones de WebEx. El organizador controla la experiencia de la reunión y, como presentador inicial, puede otorgar privilegios de presentador a los asistentes. El organizador puede iniciar la parte de conferencia de audio de una sesión, así como bloquear una reunión y expulsar a los asistentes.

Organizador alternativo

El organizador nombra un organizador alternativo. El organizador alternativo puede iniciar una reunión planificada de WebEx en vez del organizador. El organizador alternativo dispone de los mismos privilegios que el organizador y puede controlar la reunión si el organizador no está disponible.

Presentador

El presentador comparte presentaciones, aplicaciones específicas o todo el escritorio. El presentador controla las herramientas de anotación y puede otorgar o revocar el control remoto de las aplicaciones compartidas y escritorio a asistentes individuales.

Asistente

El asistente tiene una responsabilidad mínima y normalmente ve el contenido de la sesión.

La infraestructura Cisco Collaboration Cloud

La Cisco Collaboration Cloud es una infraestructura de comunicaciones diseñada con el objetivo de lograr comunicaciones en tiempo real. Los centros de datos situados estratégicamente cerca de los principales puntos de acceso a Internet emplean especialidades de gran ancho de banda con objeto de enrutar el tráfico por todo el mundo.

Arquitectura de conmutadores

Cisco emplea una red única, especializada y de distribución global de conmutadores de reuniones de alta velocidad. Los datos de la sesión de reunión creada por el ordenador del presentador y que llegan a los ordenadores de los asistentes se conmutan (nunca se almacenan de forma permanente) mediante la Cisco Collaboration Cloud. La Cisco Collaboration Cloud ofrece una infraestructura de reuniones de gran disponibilidad, con seguridad única y gran capacidad de ampliación.



Centros de datos

Las sesiones de reuniones de WebEx usan equipos de conmutación situados en múltiples centros de datos de todo el mundo. Cisco es propietario y se encarga de toda la infraestructura que se emplea en la Cisco Collaboration Cloud. Actualmente, esta red está formada por los centros de datos de Mountain View, California;Thornton, Colorado;Richardson, Texas;Ashburn, Virginia;Londres, Reino Unido;Bangalore, India;Pekín, China;y Tokio, Japón. Además, Cisco opera cuatro iPoPs (ubicaciones de puntos de presencia de red) que facilitan las conexiones troncales, el peering de Internet y las tecnologías de almacenamiento en caché para mejorar el rendimiento del usuario final y la disponibilidad. Las iPoPs se encuentran en San Jose, California; New York City, Nueva York;Bombay, India;y Melbourne, Australia. El personal de Cisco está disponible las 24 horas 7 días a la semana para ofrecer la seguridad logística necesaria, y el apoyo operativo y de gestión de cambios.

La experiencia de reuniones seguras de WebEx

Configuración del sitio de la reunión de WebEx

El módulo WebEx Site Administration gestiona y refuerza las políticas de seguridad de su sitio de WebEx personalizado. Las configuraciones controladas a este nivel determinan los privilegios del organizador y presentador en reuniones planificadas. Por ejemplo, puede deshabilitar la capacidad de un presentador de compartir aplicaciones o de transferir archivos según sitio y usuario mediante la personalización de las configuraciones de la sesión para cumplir con los objetivos comerciales y los requisitos de seguridad. El módulo WebEx Site Administration gestiona estas características relacionados con la seguridad:

Gestión de cuentas

- Bloquear una cuenta tras un número configurable de intentos de inicio de sesión fallidos.
- Desbloquear de forma automática una cuenta bloqueada tras un intervalo de tiempo específico.
- Desactivar cuentas tras un período definido de inactividad.

Acciones de gestión de cuentas de usuarios específicos

- Requerir al usuario que cambie la contraseña en el siguiente inicio de sesión.
- Bloquear o desbloquear una cuenta de usuario.
- Activar o desactivar una cuenta de usuario.

Creación de cuentas

- Requerir una confirmación de correo electrónico de las cuentas nuevas.
- Requerir texto de seguridad en nuevas solicitudes de cuentas.
- Permitir un autoregistro (darse de alta) de cuentas nuevas.
- Configurar normas para el autoregistro de cuentas nuevas.

Contraseñas de cuentas

- Reforzar los fuertes criterios de contraseñas de cuentas.
- Configurar el número de días antes de que caduque una contraseña temporal.
- Requerir al organizador que cambie las contraseñas de cuentas a un intervalo configurable.
- Requerir a todos los organizadores que cambien la contraseña de la cuenta en el próximo inicio de sesión.

Fuertes criterios de contraseñas de cuentas

- Longitud mínima.
- Mayúsculas y minúsculas.
- Mínimo de caracteres numéricos.
- Mínimo de caracteres alfabéticos.
- Mínimo de caracteres especiales.
- No permitir que un carácter se repita tres veces o más.
- No permitir volver a emplear un número específico de contraseñas previas.
- No permitir un texto dinámico (nombre del sitio, nombre del organizador, nombre de usuario).
- No permitir contraseñas de una lista configurable (por ejemplo, "contraseña").
- Intervalo mínimo de cambio de contraseña.

Fuertes criterios de contraseñas de reunión

- Requerir que todas las reuniones dispongan de contraseña.
- Longitud mínima.
- Mayúsculas y minúsculas.
- Mínimo de caracteres numéricos.
- Mínimo de caracteres alfabéticos.
- Mínimo de caracteres especiales.
- No permitir que un carácter se repita tres veces o más.
- No permitir un texto dinámico (nombre del sitio, nombre del organizador, nombre de usuario, tema de la reunión).
- No permitir contraseñas de una lista configurable (por ejemplo, "contraseña").

Salas de reunión personales: accesibles empleando una URL personalizada y una contraseña - ayudan a habilitar a que el organizador enumere las reuniones planificadas y en progreso, inicie reuniones o se una a ellas, y comparta archivos con los asistentes a la reunión. Puede emplear al administrador del sitio para fijar las características relacionadas con seguridad de sus salas de reunión personales.

- Cambiar la URL de la sala de reunión personal.
- Configurar opciones para compartir archivos en la sala de reunión personal.
- Configurar requisitos de contraseñas para archivos en la sala de reunión personal.

Otras características relacionadas con la seguridad se activan mediante la administración del sitio de WebEx.

- Permitir que cualquier organizador o asistente elija guardar su nombre y dirección de correo electrónico para lograr que unirse a reuniones sucesivas sea más fácil.
- Permitir a los organizadores reasignar registros a otros organizadores.
- Sitio de acceso restringido: el administrador del sitio puede requerir autenticación para el acceso de todos los organizadores y asistentes. La autenticación es necesaria incluso para acceder a cualquier información del sitio (como reuniones enumeradas), así como para acceder a las reuniones del sitio.
- Requerir fuertes contraseñas de reuniones para las sesiones de Cisco WebEx Remote Access.
- Requerir que todas las reuniones no aparezcan enumeradas.

Puede solicitar configuraciones adicionales de su representante de WebEx Customer Success.

- Requerir consentimiento de la solicitud "Contraseña olvidada".
- Requerir que el administrador del sitio restablezca contraseñas de cuentas, en lugar de tener que introducirlas en nombre del usuario.
- Guardar contraseñas utilizando funciones hashing unidireccionales.

Opciones de seguridad para planificar reuniones de WebEx

Dar a los organizadores individuales la capacidad de especificar la seguridad de acceso a la reunión (dentro de los parámetros configurados en la administración del sitio), que no se puede invalidar.

- Planificar una reunión como no enumerada de forma que no se muestre en el calendario visible.
- Permitir a los asistentes que se unan a las reuniones antes que el organizador.
- Permitir a los asistentes que se unan a una conferencia de audio antes que el organizador.
- Mostrar la información de la teleconferencia en la reunión.
- Finalizar reuniones de forma automática a una hora configurable en caso de que sólo quede un asistente.
- Incluir una clave de organizador en los correos electrónicos de reuniones.
- Requerir a los asistentes que introduzcan su dirección de correo electrónico cuando se unan a reuniones.

Reuniones enumeradas o no enumeradas

Los organizadores pueden optar por enumerar una reunión en el calendario público de reuniones en su sitio de WebEx personalizado. O pueden planificar la reunión como no enumerada, de forma que nunca aparezca en el calendario de reuniones. Las reuniones no enumeradas requieren que el organizador informe a los asistentes de forma explícita de la existencia de una reunión – bien a través de un enlace que se envía a los asistentes usando un proceso de invitación por correo electrónico, o requiriendo al asistente que entre en el número de reunión adjunto en la página Unirse a reuniones.

Reuniones internas o externas

Los organizadores sólo pueden restringir a aquellos asistentes con una cuenta en el sitio de WebEx personalizado, tal y como se verifica gracias a su posibilidad de iniciar sesión en el sitio para unirse a la reunión.

Contraseñas para reuniones

Un organizador puede fijar una contraseña de reunión y posteriormente de forma opcional elegir incluir o excluir la contraseña en el correo electrónico de invitación a la reunión.

Inscripción

- Restringir el acceso a la reunión con la opción de inscripción. El organizador genera una " lista de control de acceso" permitiendo el acceso sólo a los asistentes que se han inscrito y han sido aprobados explícitamente por el organizador para unirse.
- Asumir el control sobre la distribución de la información de acceso a la reunión mediante el rechazo del envío de invitaciones a la reunión por correo electrónico.
- Asegurar reuniones bloqueando la reutilización de las ID de registro en las versiones WBS27 de WebEx Training Center y WebEx Event Center. Se evitará que se una a la reunión cualquier asistente que intente reutilizar una ID de registro ya en uso.

Además, el organizador puede mantener la seguridad de la reunión restringiendo el acceso y expulsando a asistentes.

Reuniones de WebEx mejoradas mediante el uso de cualquier combinación de estas opciones planificadas para apoyar sus políticas de seguridad.

Iniciar y unirse a una reunión de WebEx

Una reunión de WebEx se inicia cuando la ID de usuario del organizador y contraseña se autentican por parte de el sitio de WebEx personalizado. El organizador dispone del control inicial de la reunión y es el presentador inicial. El organizador puede otorgar o revocar los permisos de organizador o presentador a cualquier asistente, expulsar a asistentes seleccionados o terminar la sesión en cualquier momento.

El organizador puede nombrar un organizador alternativo para iniciar y controlar la reunión en caso que el organizador no pueda asistir o pierda su conexión con la reunión. Esto hace que las reuniones sean más seguras al eliminar la posibilidad de que el papel del organizador se asigne a un asistente inesperado y no autorizado.

Puede configurar su sitio WebEx personalizado para permitir a los asistentes unirse a la reunión - incluyendo la parte de audio - antes que el organizador, y limitar las características disponibles a los primeros en unirse para hablar y el audio.

Cuando un asistente se une a una reunión de WebEx por primera vez, la aplicación de WebEx descarga de forma automática un conjunto de archivos completos en el ordenador del asistente. VeriSign emite certificados de seguridad con firma digital a dichas descargas, por lo que el asistente sabe que los archivos proceden de WebEx. En reuniones posteriores, la aplicación de WebEx descarga únicamente archivos que contengan modificaciones o actualizaciones. Los asistentes pueden emplear la función Desinstalar que ofrece el sistema operativo de su ordenador para eliminar de forma fácil todos los archivos de WebEx.

La Cisco Collaboration Cloud protege cada sesión de reunión, así como los datos dinámicos compartidos en esta.

Tecnologías de cifrado

Las reuniones de WebEx están diseñadas para ofrecer contenido multimedia sofisticado en tiempo real de forma segura a todos los asistentes dentro de una sesión de reuniones de WebEx. Cuando un presentador comparte un documento o una presentación, Universal Communications Format (UCF), una tecnología propiedad de Cisco, codifica y optimiza los datos que se van a compartir. La aplicación de reuniones de WebEx para dispositivos móviles como iPad, iPhone y BlackBerry emplea mecanismos de cifrado similares a los del PC cliente.

Las reuniones de WebEx permiten ofrecer estos mecanismos de cifrado:

1. En reuniones de WebEx a las que se asiste por ordenador o por dispositivos móviles, los datos fluyen desde el cliente a la Cisco Collaboration Cloud a través de conexiones de 128 bits de protocolo de capa de conexión segura versión 3 (SSLv3).
2. Todos los documentos y presentaciones se cifran con el estándar de cifrado avanzado (AES) de 256 bits antes de su traslado.
3. El cifrado total (E2E) es una opción que ofrecen la versión WBS26 de Cisco WebEx Meeting Center versión y superiores. Este método cifra todo el contenido de la reunión, totalmente, entre los participantes en la reunión, con el estándar de cifrado AES con una clave de 256 bits generada aleatoriamente en el ordenador del organizador y distribuida a los asistentes con un mecanismo público basado en claves.
4. El cifrado total basado en infraestructura de clave pública (PKI) es una opción que ofrecen la versión WBS27 de WebEx Meeting Center y superiores, mediante el estándar de cifrado AES de 256 bits. El mecanismo exige que los asistentes dispongan de un certificado X.509 para iniciar una reunión o unirse a ella.
5. La contraseña de inicio de sesión de un usuario para las reuniones de WebEx en dispositivos móviles está cifrada con el estándar de cifrado de datos (DES) de 128 bits.

Los administradores del sitio y los organizadores pueden seleccionar bien E2E o PKI con la opción " Tipo de reunión". Las soluciones E2E y PKI ofrecen una mayor seguridad que la AES sólo (aunque E2E y PKI asimismo emplean AES para el cifrado de carga útil) ya que la clave sólo la conocen el organizador de la reunión y los asistentes.

Cada conexión de reunión de WebEx debe autenticarse debidamente antes de establecer una conexión con la Cisco Collaboration Cloud para unirse a una reunión de WebEx. El proceso de autenticación del cliente usa una cookie única por sesión y cliente para confirmar la identidad de cada asistente que intente unirse a una reunión de WebEx. Cada reunión contiene un conjunto de parámetros de sesión generados por la Cisco Collaboration Cloud. Cada asistente autenticado debe disponer de acceso tanto a los parámetros de esta sesión como la cookie única de sesión para unirse con éxito a la reunión.

Seguridad de capa de transporte

Además de las salvaguardas de capa de la aplicación, todos los datos de la reunión se transportan usando SSLv3 de 128 bits. En lugar de emplear un puerto 80 de cortafuegos (tráfico de Internet estándar HTTP) para atravesar el cortafuegos, SSL emplea el puerto 443 del cortafuegos (tráfico HTTPS) restringiendo el acceso al puerto 80 sin afectar al tráfico WebEx.

Los asistentes a una reunión de WebEx se conectan a la Cisco Collaboration Cloud con una conexión lógica en las capas de aplicación/presentación/sesión. No existe una conexión punto a punto entre los ordenadores de los asistentes.

Compatibilidad de cortafuegos

La aplicación de reuniones de WebEx se comunica con la Cisco Collaboration Cloud para establecer una conexión segura y fiable usando HTTPS (puerto 443), de forma que los cortafuegos no tengan que estar configurados de manera específica para activar las reuniones de WebEx.

Almacenamiento de datos posterior a la reunión

No se conserva ninguna información de la sesión ni en la Cisco Collaboration Cloud ni en los ordenadores de los asistentes una vez que concluye la reunión de WebEx. Cisco conserva sólo dos tipos de información de la reunión.

- **Registros de detalles de eventos (EDR):** Cisco emplea EDR para informes y facturación. Puede ver la información de los detalles del evento en su sitio de WebEx personalizado iniciando sesión con la ID del organizador. Una vez autenticado, puede descargar estos datos desde su sitio de WebEx o acceder a este a través de WebEx APIs.
- **Archivos de grabación basada en red (NBR):** En caso de que un organizador elija grabar una sesión de reunión de WebEx, se guardará la grabación dentro de la Cisco Collaboration Cloud y puede acceder a ella través de la zona Mis Grabaciones en su sitio de WebEx.

Single Sign On (Inicio de sesión único)

Cisco es compatible con la autenticación federada para sesión única de usuarios (SSO) mediante los protocolos SAML 1.1, 2.0, y WS-Fed 1.0. El uso de autenticación federada requiere que cargue un certificado de clave pública X.509 en su sitio de WebEx personalizado. Posteriormente, generará afirmaciones SAML que contienen los atributos de usuario y firmará digitalmente las aseveraciones con la clave privada correspondiente. WebEx valida la firma de la afirmación SAML frente al certificado de clave pública cargado previamente antes de autenticar al usuario.

Informes de terceros

Más allá de sus estrictos procedimientos internos, la Oficina de seguridad de WebEx obliga a múltiples terceras personas independientes a realizar rigurosas auditorías frente a políticas internas, procedimientos y aplicaciones. Estas auditorías están diseñadas para validar requerimientos de seguridad críticos tanto para aplicaciones comerciales como gubernamentales.

Entre los auditores se incluyen Information Security Partners, LLC (iSEC Partners) que garantiza un enrutamiento de red y de aplicación exhaustiva, y PriceWaterhouseCoopers, que lleva a cabo la auditoría de controles SAS-70 Tipo II.

Enrutamiento de red iSEC

iSEC Partners ha realizado una amplia variedad de pruebas para confirmar el enrutamiento desde y hacia los asistentes a las reuniones de WebEx y la Cisco Collaboration Cloud. Estas pruebas cubren las señales de servidores de producción WebEx y las señales de confirmación de enrutamiento para diversas configuraciones de dispositivos de red que incluyen routers, cortafuegos y balanceadores de carga. Los resultados de estas pruebas indican que la comunicación de los sitios de WebEx de Estados Unidos no se establece fuera de los EE. UU. Para obtener más información, puede solicitar una copia de este informe de la oficina de seguridad de WebEx.

Revisión de código fuente iSEC

iSEC Partners realiza pruebas de penetración asistidas de código en profundidad y evaluaciones de servicio. Durante estos compromisos, iSEC Partners recibe acceso a los servicios de WebEx, código fuente y personal de ingeniería. A diferencia de las pruebas de la caja negra, este alto grado de acceso permite a iSEC Partners:

- Identificar aplicaciones críticas y vulnerabilidades del servicio y proponer soluciones.
- Recomendar áreas generales para la mejora de la arquitectura.
- Identificar errores de códigos y ofrecer asistencia para las mejoras de prácticas de códigos.
- Trabajar directamente con el personal de ingeniería de WebEx para explicar los descubrimientos y ofrecer asistencia para un trabajo de solución.

Para obtener más información, puede solicitar una copia de este informe a la oficina de seguridad de WebEx.

SAS-70 Tipo II

PricewaterhouseCoopers LLP realiza una auditoría anual SAS-70 Tipo II según los estándares establecidos por la AICPA. Para obtener más información sobre el estándar SAS-70, consulte: www.sas70.com/index2.htm. Para obtener más información, puede solicitar una copia del informe de PricewaterhouseCoopers LLP SAS-70 a la oficina de seguridad de WebEx a través de su representante de cuentas de Cisco.

ISO-27001/2

Cisco diseñó los controles SAS70 con el fin de que se parecieran a los controles de seguridad de información de la norma ISO27002, a la que se hace referencia en un apéndice de la ISO27001. La norma ISO-27001 es un estándar de seguridad de información publicado por la Organización Internacional de Normalización (ISO) que proporciona recomendaciones sobre las mejores prácticas en la creación de un sistema de gestión de seguridad de la información (SGSI). Un SGSI es un marco de políticas y procedimientos que incluye todos los controles legales, físicos y técnicos implicados en los procesos de gestión de riesgos de la información de una organización. De acuerdo con su documentación, la ISO 27001 se desarrolló para "ofrecer un modelo de establecimiento, implementación, operación, control, revisión, conservación y mejora de un sistema de gestión de la seguridad de la información. Para obtener más información sobre la ISO-27001/2, consulte el siguiente enlace: <http://www.27000.org/>.

Conclusión

Su organización puede confiar en las aplicaciones en línea de Cisco WebEx para activar la colaboración y agilizar los procesos empresariales, incluso en los entornos de seguridad más estrictos. Elija las soluciones de colaboración Software-as-a-Service fáciles de usar, fiables, probadas y seguras de WebEx, Cisco.

