Informe técnico

Conferencias web: Aproveche el potencial de la colaboración segura y en tiempo real

Este documento se centra en la información de seguridad de Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center y Cisco WebEx Event Center.

Introducción

Las soluciones online de Cisco WebEx® hacen posible que los empleados globales y los equipos virtuales se conozcan y colaboren en tiempo real como si estuvieran trabajando en la misma sala. De hecho, la colaboración online puede ser aún más beneficiosa que la colaboración cara a cara tradicional ya que elimina los problemas que pueden causar el tiempo y los gastos de desplazamiento, o incluso la falta de espacio en las instalaciones. Las empresas, las instituciones y las agencias gubernamentales de todo el mundo confían en las soluciones Cisco WebEx® para simplificar los procesos empresariales y mejorar los resultados de las ventas, el marketing, la formación, la gestión de proyectos y los equipos de soporte.

Para todas estas empresas y organismos, la seguridad es una cuestión fundamental. La colaboración online debe proporcionar varios niveles de seguridad, desde la programación de las reuniones hasta la autenticación de los participantes a la hora de utilizar documentos compartidos.

Cisco hace de la seguridad su mayor prioridad en el diseño, implantación y mantenimiento de su red, plataforma y aplicaciones. Puede introducir soluciones WebEx® en sus procesos empresariales con total confianza, incluso con los requisitos de seguridad más estrictos.

Una de las partes más importantes a la hora de planificar su inversión es comprender bien las funciones de seguridad de las aplicaciones online y la infraestructura de comunicación subyacente, es decir, la nube de Cisco WebEx.

La infraestructura de la nube de Cisco WebEx

Cisco WebEx Meetings es una solución de software como servicio (SaaS) que ofrece la nube de Cisco WebEx, una plataforma segura de prestación de servicios, cuyo rendimiento, integración, flexibilidad, escalabilidad y disponibilidad es líder en el sector. La nube de Cisco WebEx representa un modo fácil de implementar y suministrar aplicaciones para reducir el coste total de propiedad y mantener al mismo tiempo el grado máximo de seguridad empresarial.

Arquitectura basada en switches

Cisco emplea una red exclusiva y de distribución global de switches de conferencias de alta velocidad. Los datos de la reunión que se originan en el equipo del presentador y que llegan a los equipos de los participantes se conmutan (no se almacenan de manera persistente) a través de la nube de Cisco WebEx.[1]

[1] Cuando el usuario habilita la grabación basada en la red (Network-based recording, NBR) la reunión se graba y se almacena. Además de NBR, WebEx también almacena datos del perfil y de los archivos de los usuarios.

Data Centers

La nube de Cisco WebEx es una infraestructura de comunicaciones diseñada con el objetivo de lograr comunicaciones web en tiempo real. Las sesiones de las reuniones WebEx usan equipos de switching situados en varios Data Centers de todo el mundo. Estos Data Centers están situados estratégicamente cerca de los principales puntos de acceso a Internet y emplean fibra exclusiva de gran ancho de banda con objeto de enrutar el tráfico por todo el mundo. Cisco gestiona toda la infraestructura en la nube de Cisco WebEx. Los datos de los Estados Unidos permanecen en la región de EE. UU. y los datos de Europa en la zona europea.

Además, Cisco gestiona las ubicaciones de punto de presencia (point-of-presence, PoP) de red que facilitan las conexiones de red troncal, el peering de Internet y las tecnologías de almacenamiento del sitio global y en caché para mejorar el rendimiento del usuario final y la disponibilidad. El personal de Cisco está disponible las 24 horas del día, los 7 días de la semana, para ofrecer soporte logístico de seguridad, operativo y de gestión de cambios.

Descripción general de las reuniones altamente seguras de WebEx

Las reuniones a través de WebEx incluyen:

- Configuración del lugar de la reunión
- Opciones de seguridad para la programación
- Opciones para iniciar y unirse a una reunión WebEx
- Tecnologías de cifrado
- Seguridad de la capa de transporte
- Compatibilidad con firewalls
- Privacidad de datos de la reunión
- Seguridad dentro de la reunión
- Inicio de sesión único
- Acreditaciones de terceros (auditorías independientes que demuestran la seguridad que ofrece Cisco WebEx)

Los términos "reuniones con Cisco WebEx" y "sesiones de reunión con Cisco WebEx" hacen referencia a los servicios de conferencias con audio integrado, teléfono a través de Internet y videoconferencias desde un único punto y desde varios puntos que se emplean en todos los productos online de Cisco WebEx. Algunos de estos productos son:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center (incluidos 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 de WebEx mencionadas anteriormente.

Funciones en las reuniones WebEx

Las cuatro funciones que una persona puede desempeñar en una reunión WebEx son: organizador, organizador alternativo, presentador y asistente. Las siguientes secciones describen los privilegios en cuanto a seguridad de cada función.

Organizador

El organizador planifica e inicia las reuniones WebEx. El organizador es quien gestiona la reunión. Desde el punto de vista de la seguridad, el organizador puede otorgar privilegios de presentador a los asistentes. El organizador también puede bloquear la reunión y expulsar a asistentes.

Organizador alternativo

El organizador designa a un organizador alternativo, que puede iniciar una reunión WebEx programada en lugar del organizador. Desde el punto de vista de la seguridad, el organizador alternativo tiene los mismos privilegios que el organizador.

Presentador

El presentador comparte las presentaciones, las aplicaciones específicas o todo el escritorio. El presentador controla las herramientas de anotación. Desde el punto de vista de la seguridad, el presentador puede conceder y anular el control sobre las aplicaciones compartidas y el escritorio a los participantes individuales.

Asistente

Un asistente no tiene responsabilidades de seguridad ni privilegios.

Módulo WebEx Site Administration

El módulo WebEx Site Administration permite a los administradores autorizados gestionar y aplicar políticas de seguridad en cada reunión para conceder los privilegios de organizador y de presentador. Por ejemplo, puede personalizar las configuraciones de sesión para deshabilitar la función del presentador con el fin de compartir aplicaciones o transferir archivos por sitio o por usuario.

El módulo WebEx Site Administration gestiona estas características relacionados con la seguridad:

Gestión de cuentas

- Bloquea una cuenta tras un número configurable de intentos de inicio de sesión fallidos.
- Desbloquea de forma automática una cuenta bloqueada tras un intervalo de tiempo específico.
- Desactiva cuentas tras un período definido de inactividad.

Acciones específicas de cuenta de usuario

- Solicita al usuario que cambie la contraseña en el siguiente inicio de sesión.
- Bloquea o desbloquea cuentas de usuario.
- Activa o desactiva cuentas de usuario.

Creación de cuentas

- Requiere un texto de seguridad en solicitudes de cuentas nuevas.
- Solicita una confirmación de correo electrónico en las cuentas nuevas.
- Permite el autorregistro para cuentas nuevas.
- Configura reglas para el autorregistro de cuentas nuevas.

Contraseñas de las cuentas

Refuerza los sólidos criterios de las contraseñas de las cuentas.

- Combinación de mayúsculas y minúsculas.

- Longitud mínima.
- Número mínimo de caracteres numéricos.
- Número mínimo de caracteres alfabéticos.
- Número mínimo de caracteres especiales.
- Sin caracteres que se repitan tres veces o más.
- No reutiliza un número determinado de contraseñas anteriores.
- Sin texto dinámico (nombre del sitio, nombre del organizador, nombre de usuario).
- Sin contraseñas de una lista configurable (por ejemplo, "contraseña").
- Intervalo de tiempo mínimo antes de cambiar la contraseña.
- Cambio de la contraseña de la cuenta del organizador en un intervalo de tiempo configurable
- Cambio de las contraseñas de las cuentas de todos los usuarios en la siguiente sesión

Salas personales de reuniones

Es posible acceder a las salas personales de reuniones mediante una dirección URL o contraseña personalizadas. En dichas salas, el organizador puede buscar las reuniones planificadas o que estén en curso, iniciar o unirse a reuniones y compartir archivos con los asistentes a alguna de ellas. Los administradores pueden configurar funciones relacionadas con la seguridad en las salas de reuniones personales, como:

- Opciones para compartir archivos
- Requisitos de contraseñas para archivos

Otras características relacionadas con la seguridad que se activan mediante WebEx Site Administration

- El organizador o los asistentes pueden guardar los nombres y direcciones de correo electrónico para que sea más fácil organizar o unirse a las nuevas reuniones.
- Los organizadores pueden reasignar grabaciones a otros organizadores.
- El acceso al sitio se puede restringir solicitando una autenticación para cada acceso de organizador y asistente. Se puede solicitar la autenticación para acceder a cualquier información del sitio, como la lista de reuniones, así como acceder a las reuniones del sitio.
- Las reglas de contraseñas seguras se pueden aplicar a WebEx Access Anywhere.
- Todas las reuniones se pueden ocultar de la lista.
- Se puede requerir aprobación para las solicitudes del tipo "¿Olvidó su contraseña?"
- Se puede requerir que se restablezcan las contraseñas de las cuentas en lugar de volver a introducirlas en nombre de los usuarios.

Opciones de seguridad para planificar reuniones WebEx

- Los organizadores individuales pueden tener la capacidad de especificar el tipo de seguridad de acceso a la reunión (dentro de los parámetros configurados en el nivel de la administración del sitio que no se pueden invalidar).
- Una reunión puede ocultarse de la lista para que no aparezca en el calendario visible.
- Los asistentes pueden entrar en las reuniones antes de que lo haga el organizador.
- Los asistentes pueden acceder al audio antes de que el organizador se una a la reunión.

- Solo los asistentes que posean una cuenta para el sitio WebEx pueden unirse.
- En las reuniones puede mostrarse la información sobre la teleconferencia.
- Las reuniones pueden finalizar automáticamente en el momento que se configure si solo queda un asistente.
- Se puede solicitar a los asistentes que introduzcan su dirección de correo electrónico cuando se unan a las reuniones

Reuniones en la lista u ocultas

Los organizadores pueden decidir que la reunión aparezca en el calendario público de reuniones en el sitio WebEx personalizado. También pueden planificar la reunión como oculta, de forma que nunca aparezca en el calendario de reuniones. En las reuniones ocultas, el organizador debe informar de forma explícita de la existencia de una reunión, bien a través de un enlace que se envía a los asistentes mediante el proceso de invitación por correo electrónico o bien solicitando al asistente que entre en el número de reunión que aparece en la página de inicio de las reuniones.

Reuniones internas o externas

Los organizadores solo pueden restringir la reunión a aquellos asistentes que tengan una cuenta en el sitio WebEx personalizado. Esto se comprueba cuando inician sesión para incorporarse a la reunión.

Contraseñas de la reunión

Un organizador puede establecer una contraseña de reunión y posteriormente decidir si indicar o no la contraseña en el correo electrónico de invitación a la reunión.

Inscripción

- El organizador puede restringir el acceso con la función de registro. El organizador genera una "lista de control de acceso" que permite el acceso solo a los asistentes que se han inscrito y han recibido la aprobación explícita del organizador para poder unirse.
- Las reuniones son seguras ya que se bloquea el uso posterior de las ID de registro en WebEx Training Center y WebEx Event Center. Así, se evitará que se incorpore a la reunión cualquier asistente que intente reutilizar una ID de registro ya en uso. Esto impide que varios asistentes compartan una misma ID.
- Además, el organizador puede mantener la seguridad de la reunión restringiendo el acceso y expulsando a asistentes.

Cualquier combinación de estas opciones de programación puede ajustarse para cumplir con las políticas de seguridad.

Abrir y unirse a una reunión WebEx

Una reunión WebEx comienza cuando la ID de usuario y la contraseña del organizador se autentican desde el sitio WebEx personalizado. El organizador es quien toma inicialmente el control de la reunión y asume la función de presentador. El organizador puede otorgar o revocar los permisos de organizador o presentador a cualquier asistente, expulsarlos o dar por finalizada la sesión en cualquier momento.

El organizador puede nombrar a un organizador alternativo para iniciar y gestionar la reunión en caso que 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 (y acceder al audio) antes que el organizador, así como limitar las funciones disponibles para los primeros en unirse para hablar y su audio.

Cuando un asistente se une a una reunión WebEx por primera vez, el software cliente de WebEx se descarga y se instala automáticamente en el equipo del asistente. El software cliente de WebEx se firma digitalmente con un certificado que publica VeriSign. En reuniones posteriores, la aplicación WebEx solo descarga e instala los 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 los archivos de WebEx.

Tecnologías de cifrado

Las reuniones WebEx están diseñadas para ofrecer contenido multimedia complejo en tiempo real y de forma segura a todos los asistentes dentro de una sesión de reunión WebEx. Cuando el presentador comparte un documento o una presentación, estos se codifican mediante el formato universal UCF (Universal Communications Format), una tecnología patentada de Cisco® que optimiza los datos para el uso compartido. La aplicación de reuniones WebEx para dispositivos móviles como iPad, iPhone y BlackBerry emplea mecanismos de cifrado similares a los del cliente del PC.

Las reuniones WebEx ofrecen estos mecanismos de cifrado:

- En reuniones WebEx a las que se asiste a través de un ordenador o un dispositivo móvil, los datos fluyen desde el cliente a la nube de Cisco WebEx a través de conexiones con protocolo de capa de conexión segura (SSL) de 128 bits.
- Cisco WebEx Meeting Center ofrece la opción de cifrado de extremo a extremo (E2E). Este método cifra todo el contenido de la reunión, de extremo a extremo, entre todos los participantes, gracias al estándar de cifrado avanzado (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. A diferencia del cifrado SSL, que termina en la nube de Cisco WebEx, el cifrado E2E incluye todo el contenido de la reunión dentro de la infraestructura de nube de Cisco WebEx. Los datos del contenido de la reunión sin cifrar aparecen solo en la memoria de los ordenadores de los participantes de la reunión.[2]
- Si un usuario decide utilizar la opción "Recordarme" relacionada, la ID y la contraseña del usuario para las reuniones WebEx que se hayan almacenado en el ordenador y en los dispositivos móviles se cifran mediante el AES de 128 bits.

Los administradores del sitio y los organizadores pueden elegir el cifrado E2E con la opción "Tipo de reunión". La solución E2E ofrece una mayor seguridad que solo con la AES (aunque el cifrado E2E también usa AES para el cifrado de carga útil) ya que la clave solo la conocen el organizador de la reunión y los asistentes.

Cada conexión desde el cliente de reuniones de WebEx hasta la nube de WebEx se autentica con un token criptográfico, de modo que solo los usuarios legítimos pueden incorporarse a una reunión concreta.

Seguridad de la capa de transporte

Además de la protección de la capa de aplicación, todos los datos de la reunión se transportan usando el SSL de 128 bits. En lugar de emplear el puerto 80 del firewall (que se utiliza para el tráfico de Internet estándar HTTP) para atravesar el firewall, SSL emplea el puerto 443 (empleado para el tráfico HTTPS).

---

[2] Tenga en cuenta que NBR no está disponible cuando se habilita el cifrado E2E. Esta opción solo está disponible para WebEx Meeting Center.

Los asistentes a una reunión WebEx se conectan a la nube de Cisco WebEx mediante una conexión lógica en las capas de aplicación/presentación/sesión. No existe una conexión punto a punto entre los equipos de los asistentes.

Compatibilidad del firewall

La aplicación de reuniones WebEx se comunica con la nube de Cisco WebEx para establecer una conexión fiable y altamente segura mediante HTTPS (puerto 443). Por ese motivo, los firewalls no tienen que estar configurados especialmente para habilitar las reuniones de WebEx.

Privacidad de datos de la reunión

Todo el contenido de las reuniones WebEx (conversación, audio, vídeo, escritorio o documentos compartidos) son transitorios (solo existen durante la reunión). El contenido de la reunión no se almacena ni en la nube de Cisco ni en el equipo de un asistente de forma predeterminada. Cisco solo guarda dos tipos de información de la reunión, que son:

- **Registros de detalles del evento (EDR):** Cisco utiliza EDR para realizar la facturación y los informes. Puede ver la información de los detalles del evento en su sitio WebEx personalizado iniciando sesión con su ID de organizador. Una vez autenticado, puede descargar estos datos desde su sitio WebEx o acceder a este a través de la API de WebEx. Los EDR contienen información básica sobre la asistencia a la reunión, como por ejemplo quién asiste (nombre y correo electrónico del usuario), a qué reunión (ID de reunión) y cuándo (hora de inicio y finalización de la conexión).
- **Archivos de grabación basada en la red (NBR):** En caso de que un organizador decida grabar una sesión de WebEx, la grabación se guardará dentro de la nube de Cisco WebEx y se podrá acceder a ella través de la sección Mis Grabaciones en su sitio WebEx. El archivo se creará solo en caso de que el organizador habilite el NBR durante la reunión o seleccione una opción de "sitewide" para grabar todas las reuniones. Se puede acceder a los NBR a través de enlaces de URL. Cada enlace contiene un token impredecible. El organizador tiene pleno control del acceso a los archivos NBR, incluida la capacidad de suprimirlo, compartirlo o agregar una contraseña para protegerlo. La función de NBR es optativa y el administrador puede deshabilitarla.

Inicio de sesión único

Cisco admite la autenticación federada para inicio de sesión único (SSO) con un Lenguaje de marcado de aserción de seguridad (SAML) 1.1 y 2.0 y los protocolos 1.0 de la WS-Federation. Se ha eliminado la compatibilidad con SAML 1.1. Para usar la autenticación federada debe cargar un certificado de clave pública X.509 en su sitio WebEx personalizado. Posteriormente, puede generar aserciones SAML que contengan los atributos de usuario y firmar digitalmente las aserciones 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 contrata a varias empresas externas para realizar rigurosas auditorías de políticas internas, procedimientos y aplicaciones. Estas auditorías están diseñadas para validar los requisitos de seguridad críticos tanto para aplicaciones comerciales como gubernamentales.

Evaluación de seguridad de los datos llevada a cabo por terceros

Cisco emplea empresas externas para realizar pruebas de penetración y evaluaciones continuas, detalladas y codificadas. En este contexto, una empresa externa lleva a cabo las siguientes evaluaciones de seguridad:

- Identificación de las aplicaciones críticas o las vulnerabilidades del servicio y propuesta de soluciones.
- Recomendación de áreas generales para la mejora de la arquitectura.
- Identificación de los errores de codificación y ayuda para mejorar las prácticas de codificación.
- Se trabaja directamente con el personal de ingeniería de WebEx para explicar las conclusiones y ofrecer asesoramiento para poner en marcha las soluciones.

Certificación Safe Harbor

En marzo de 2012, Cisco obtuvo la certificación Safe Harbor en relación con los datos de clientes y partners (la certificación Safe Harbor para los datos de empleados se consiguió en 2011). Esta certificación es un elemento adicional al completo programa de cumplimiento de privacidad de Cisco y, aunque no es necesario para el gobierno o el consejo normativo, la empresa reconoce el valor que los clientes le dan a esta certificación.

La Directiva de protección de datos de la UE prohíbe la transferencia de datos personales de los ciudadanos europeos a países no pertenecientes a la Unión que no cumplan el estándar de “suficiencia” para la protección de la privacidad. El Departamento de Comercio de los EE. UU., junto con la Comisión Europea, desarrolló un marco de trabajo "Safe Harbor" que permite que las organizaciones estadounidenses cumplan la Directiva respetando un conjunto de principios de privacidad "Safe Harbor". Las empresas certifican su cumplimiento con estos principios en el sitio web del Departamento de Comercio de los EE. UU. La UE aprobó el marco de trabajo en el año 2000, que permite que las empresas que cumplen con los principios logren que la UE considere sus prácticas como “adecuadas” para la protección de la privacidad de los ciudadanos de la UE.

SSAE16

PricewaterhouseCoopers realiza una declaración anual sobre estándares para la auditoría de los compromisos de la atestiguación N.º 16 (SSAE16) de acuerdo con los estándares establecidos por el instituto estadounidense de censores jurados de cuentas. Para obtener más información sobre el SSAE16 visite: http://www.ssae16.com.

ISO 27001 y 27002

Cisco obtuvo la certificación ISO 27001 para los servicios de WebEx en octubre de 2012. La certificación se renueva cada tres años con una auditoría externa provisional anual. 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, administrativos, 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". Consulte este enlace para obtener más información sobre ISO 27001 y 27002: http://www.27000.org/.

Para obtener más información

Para obtener más información sobre las soluciones de Cisco WebEx, visite http://www.cisco.com/c/es_es/products/conferencing/index.html o póngase en contacto con su representante de ventas.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Ámsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la Web de Cisco en www.cisco.com/go/offices.

Impreso en EE. UU. C11-709579-01 04/14