Informe técnico

Conferencias web: Libere el potencial de una colaboración segura en tiempo real

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

Introducción

Las soluciones en línea de Cisco WebEx® ayudan a los empleados y equipos virtuales de todo el mundo a reunirse y colaborar en tiempo real como si estuvieran en la misma sala. De hecho, la colaboración en línea puede ser mejor que la tradicional colaboración cara a cara en términos de ahorro de costos y tiempos de viaje, y problemas de espacio en la sala. Empresas, instituciones y organismos de gobierno de todo el mundo confían en las soluciones Cisco WebEx® para simplificar los procesos empresariales y mejorar los resultados de los equipos de ventas, marketing, capacitación, administración de proyectos y soporte técnico.

Para todas estas empresas y organismos, la seguridad es una preocupación fundamental. La colaboración en línea debe proporcionar varios niveles de seguridad, desde la planificación de reuniones y la autenticación de participantes hasta el uso compartido de documentos.

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

Comprender las características de seguridad de las aplicaciones en línea de Cisco WebEx y la infraestructura de comunicación subyacente, Cisco WebEx Cloud, es una parte importante de su decisión de inversión.

La infraestructura de Cisco WebEx Cloud

Cisco WebEx Meetings es una solución de software como servicio (SaaS) que se ofrece a través de Cisco WebEx Cloud, una plataforma de prestación de servicios sumamente segura que brinda el mayor nivel de rendimiento, flexibilidad, integración, escalabilidad y disponibilidad del sector. Cisco WebEx Cloud ofrece facilidad de implementación y distribución de aplicaciones para reducir el costo total de propiedad, además de garantizar el máximo nivel de seguridad de la empresa.

Arquitectura de switching

Cisco implementa una red exclusiva de switches de alta velocidad para reuniones, distribuidos en todo el mundo. Los datos de sesión de las reuniones que se originan en la computadora del presentador y llegan a las computadoras de los asistentes nunca se almacenan de manera persistente en Cisco WebEx Cloud sino que se transmiten por switches a través de esta nube.[1]

[1] Cuando el usuario habilita la grabación por red (NBR), la reunión se graba y almacena. Además de la NBR, WebEx también almacena datos de perfiles de usuarios y archivos de usuarios.

Centros de datos

Cisco WebEx Cloud es una infraestructura de comunicaciones diseñada específicamente para comunicaciones web en tiempo real. Las sesiones de reunión de WebEx emplean equipos de switching ubicados en varios centros de datos en todo el mundo. Estos centros de datos se ubican estratégicamente cerca de los puntos de acceso a Internet más importantes y utilizan fibra dedicada de alto ancho de banda para enrutar el tráfico en todo el mundo. Cisco opera toda la infraestructura dentro de Cisco WebEx Cloud. Los datos de los Estados Unidos permanecen en territorio estadounidense, mientras que los datos de Europa permanecen en territorio europeo.

Además, Cisco opera ubicaciones de puntos de presencia (PoP) de la red que facilitan conexiones troncales, interconexión por Internet, copias globales de seguridad del sitio y tecnologías de almacenamiento en caché que contribuyen a mejorar el rendimiento y la disponibilidad del usuario final. El personal de Cisco está disponible las 24 horas del día, los siete días de la semana, para proporcionar todo el soporte necesario de seguridad logística, operaciones y administración de cambios.

Descripción general de la experiencia de reunión altamente segura de WebEx

La experiencia de reunión de WebEx incluye:

- Configuración del lugar de reunión
- Opciones de seguridad para planificación
- Opciones para iniciar y entrar a una reunión de WebEx
- Tecnologías de cifrado
- (Protocolo de) Seguridad de la capa de transporte
- Compatibilidad con firewalls
- Privacidad de los datos de la reunión
- Seguridad en la reunión
- Inicio de sesión único
- Acreditaciones de terceros (auditorías independientes validan la seguridad de Cisco WebEx)

Los términos “reuniones de WebEx” y “sesiones de reunión de Cisco WebEx” se refieren a las conferencias de audio integrado, las conferencias de voz por Internet y las videoconferencias de punto único y multipunto que se utilizan en todos los productos en línea de Cisco WebEx. Estos productos incluyen:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- 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 se aplican por igual a todas las aplicaciones de WebEx mencionadas anteriormente.

Roles en las reuniones de WebEx

Los cuatro roles en una reunión de WebEx son organizador, organizador alternativo, presentador y asistente. Las siguientes secciones describen los privilegios de seguridad de cada rol.

Organizador

El organizador planifica e inicia una reunión de WebEx. El organizador controla la experiencia en las reuniones. 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 planificada de WebEx en lugar del organizador. Desde el punto de vista de la seguridad, el organizador alternativo tiene los mismos privilegios que el organizador.

Presentador

Un presentador comparte presentaciones, aplicaciones específicas o un escritorio completo. El presentador controla las herramientas de anotación. Desde el punto de vista de la seguridad, el presentador puede otorgar y revocar el control remoto de las aplicaciones y el escritorio compartidos a asistentes individuales.

Asistente

Un asistente no tiene responsabilidades ni privilegios de seguridad.

Módulo Administración del sitio de WebEx

El módulo Administración del sitio de WebEx les permite a los administradores autorizados administrar y aplicar políticas de seguridad a reuniones individuales en términos de privilegios de organizador y presentador. Por ejemplo, puede personalizar las configuraciones de la sesión para desactivar la capacidad de un presentador de compartir aplicaciones o transferir archivos según el sitio o usuario en cuestión.

El módulo Administración del sitio de WebEx permite administrar estas características relacionadas con la seguridad:

Administración de cuentas

- Bloquear una cuenta después de una cantidad determinada de intentos fallidos de inicio de sesión
- Desbloquear automáticamente una cuenta bloqueada después de un plazo específico
- Desactivar cuentas al cabo de un período de inactividad definido

Acciones para cuentas de usuario específicas

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

Creación de cuentas

- Requerir texto de seguridad para solicitudes de cuentas nuevas
- Requerir confirmación por correo electrónico de nuevas cuentas
- Permitir la inscripción automática (registro) para nuevas cuentas
- Configurar reglas para la inscripción automática de nuevas cuentas

Contraseñas de cuentas

Aplicar sólidos criterios de contraseñas para las cuentas, incluidos los siguientes:

- Uso combinado de mayúsculas y minúsculas
- Longitud mínima
- Cantidad mínima de caracteres numéricos
- Cantidad mínima de caracteres alfabéticos
- Cantidad mínima de caracteres especiales
- Prohibir la repetición de cualquier carácter tres veces o más
- Prohibir la reutilización de una cantidad específica de contraseñas anteriores
- Prohibir texto dinámico (nombre del sitio, nombre del organizador, nombre de usuario)
- Prohibir contraseñas incluidas en una lista configurable (por ejemplo, “contraseña”)
- Plazo mínimo para poder cambiar la contraseña
- Cambio de contraseña de cuenta por parte del organizador al cabo de un plazo configurable
- Cambio de contraseña de cuenta por parte de todos los usuarios en el inicio de sesión siguiente

Salas de reuniones personales

Se puede tener acceso a las salas de reuniones personales a través de una URL personalizada y una contraseña. En estas salas, el organizador puede listar reuniones planificadas y en curso, iniciar y entrar a reuniones y compartir archivos con los asistentes a la reunión. Los administradores pueden configurar características relacionadas con la seguridad para salas de reuniones personales, incluidas las siguientes:

- Opciones para compartir archivos en la sala de reuniones personales
- Solicitudes de contraseña para archivos en la sala de reuniones personales

Otras características relacionadas con la seguridad habilitadas a través del módulo Administración del sitio de WebEx

- El organizador o los asistentes pueden optar por almacenar sus nombres y direcciones de correo electrónico para que resulte más sencillo organizar o entrar a nuevas reuniones.
- Los organizadores pueden reasignar grabaciones a otros organizadores.
- El acceso al sitio puede restringirse mediante autenticación para el acceso de cualquier organizador y asistente. Se puede requerir autenticación para tener acceso a cualquier información del sitio, como reuniones listadas, y tener acceso a reuniones en el sitio.
- Se pueden aplicar reglas de contraseñas seguras a WebEx Access Anywhere.
- Todas las reuniones pueden estar no listadas.
- Se puede requerir aprobación de una solicitud “¿Olvidó su contraseña?”.
- Se puede requerir que las contraseñas de las cuentas se restablezcan en lugar de volver a ingresarlas en nombre de un usuario.

Opciones de seguridad para planificar reuniones en WebEx

- A los organizadores individuales se les puede dar la capacidad de especificar la seguridad del acceso a una reunión (dentro de parámetros configurados en el nivel de administración del sitio que no pueden anularse).
- Una reunión puede estar no listada para que no figure en el calendario visible.
- Se puede permitir a los asistentes que se unan a reuniones antes de que se una el organizador.
- Los asistentes pueden tener acceso al audio antes de que se una el organizador.
- Solo se puede permitir que los asistentes con una cuenta en el sitio de WebEx se unan.
- La información de las teleconferencias puede mostrarse en las reuniones.
- Las reuniones pueden terminar automáticamente al cabo de un período configurable si queda un solo asistente.
- Se les puede solicitar a los asistentes que introduzcan su dirección de correo electrónico cuando se unen a las reuniones.

Reuniones listadas o no listadas

Los organizadores pueden optar por listar una reunión en el calendario de reuniones públicas en un sitio personalizado de WebEx. O bien, pueden planificar la reunión como no listada, de modo que nunca aparezca en un calendario de reuniones. Las reuniones no listadas requieren que el organizador informe explícitamente a los asistentes sobre la existencia de la reunión, ya sea mediante el envío de un enlace a los asistentes con el uso del proceso de invitación por correo electrónico o solicitando al asistente que introduzca el número de reunión proporcionado en la página Join Meeting (Entrar a una reunión).

Reuniones internas o externas

Los organizadores pueden restringir las reuniones de modo que solo puedan ingresar los asistentes que tengan una cuenta en un sitio personalizado de WebEx, lo que queda verificado por su capacidad de conectarse al sitio para entrar a la reunión.

Contraseñas de reunión

El organizador puede configurar una contraseña para la reunión y luego optar por incluirla o no en el correo electrónico de invitación a la reunión.

Inscripción

- El organizador puede restringir el acceso a la reunión con la función de inscripción. El organizador genera una “lista de control de acceso” que solo admite a los invitados que se hayan inscrito y hayan sido aprobados explícitamente por el organizador.
- Las reuniones pueden asegurarse bloqueando la reutilización de la ID de inscripción en WebEx Training Center y en WebEx Event Center. Los asistentes que intenten reutilizar una ID de inscripción en uso no podrán entrar a la reunión. Esto evita el uso compartido de ID entre varios asistentes.
- Además, un organizador puede preservar la seguridad de la reunión restringiendo el acceso y expulsando participantes.

Cualquier combinación de estas opciones de planificación puede ajustarse a sus políticas de seguridad.

Inicio y acceso a una reunión de WebEx

Una reunión de WebEx comienza una vez que su sitio personalizado de WebEx autentica la ID de usuario y la contraseña de un organizador. El organizador tiene el control inicial de la reunión y es el presentador inicial. El organizador puede otorgar o revocar permisos de organizador o presentador a cualquier asistente, expulsar a asistentes determinados o finalizar la sesión en cualquier momento.

El organizador puede designar a un organizador alternativo para que inicie y controle la reunión en caso de no poder asistir o de perder la conexión con la reunión. Esta función hace las reuniones más seguras, ya que elimina la posibilidad de que se asigne el rol de organizador a un asistente no autorizado o no previsto.

Usted puede configurar su sitio personalizado de WebEx para permitir que los asistentes se unan a la reunión —incluida la recepción de audio— antes que el organizador y limitar las características disponibles para los primeros que se sumen a la conversación por chat y audio.

Cuando un asistente se une a una reunión de WebEx por primera vez, el software de cliente de WebEx se descarga e instala automáticamente en la computadora del asistente. El software de cliente de WebEx se firma digitalmente con un certificado de VeriSign. En reuniones posteriores, la aplicación de WebEx solo descarga e instala archivos que contienen cambios o actualizaciones. Los asistentes pueden utilizar la función de desinstalación proporcionada por el sistema operativo de la computadora para eliminar los archivos de WebEx de modo sencillo.

Tecnologías de cifrado

Las reuniones de WebEx están diseñadas para transmitir contenidos multimedia en tiempo real y en condiciones de seguridad a cada asistente dentro de una sesión de reunión de WebEx. Cuando un presentador comparte un documento o una presentación, el material se codifica con el formato universal de comunicaciones (UCF), una tecnología exclusiva de Cisco® que optimiza los datos para uso compartido. La aplicación para reuniones de WebEx en dispositivos móviles como iPad, iPhone y BlackBerry emplea mecanismos de cifrado similares a los del cliente para PC.

Las reuniones de WebEx proporcionan estos mecanismos de cifrado:

- Para reuniones de WebEx en computadoras y dispositivos móviles, los datos se transportan del cliente a Cisco WebEx Cloud con un cifrado Secure Sockets Layer (SSL) de 128 bits.
- El cifrado integral (E2E) es una opción que se ofrece con Cisco WebEx Meeting Center. Con este método se cifra todo el contenido de la reunión entre los participantes mediante el estándar de cifrado avanzado (AES) con una clave de 256 bits generada aleatoriamente en la computadora del organizador y distribuida entre los asistentes con un mecanismo público basado en clave. A diferencia del cifrado SSL, que finaliza del lado de Cisco WebEx Cloud, el cifrado E2E codifica todo el contenido de la reunión dentro de la infraestructura de Cisco WebEx Cloud. Los datos de contenido de texto no cifrado de la reunión se presentan únicamente en la memoria de las computadoras de los participantes.[2]
- Si un usuario elige la opción “Recordar mi usuario” relacionada, la ID de inicio de sesión y la contraseña de ese usuario para reuniones de WebEx que se guarden en computadoras y dispositivos móviles se codificarán con cifrado AES de 128 bits.

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

Los administradores del sitio y los organizadores pueden seleccionar el cifrado E2E con la opción “Tipo de reunión”. La solución E2E brinda más seguridad que si se utiliza únicamente AES (aunque el cifrado E2E también utiliza AES para el cifrado de la carga útil), ya que los únicos que conocen la clave son el organizador y los asistentes de la reunión.

Cada conexión desde el cliente de reuniones de WebEx hasta WebEx Cloud se autentica con un token criptográfico, de modo que solo los usuarios legítimos puedan entrar a una reunión específica.

Seguridad de la capa de transporte

Además de las protecciones de capa de la aplicación, todos los datos de la reunión se transportan mediante SSL de 128 bits. En lugar de atravesar el firewall por el puerto 80 (utilizado para tráfico de Internet HTTP estándar), SSL utiliza el puerto de firewall 443 (utilizado para tráfico HTTPS).

Los asistentes a las reuniones de WebEx se conectan a Cisco WebEx Cloud mediante una conexión lógica en las capas de aplicación, presentación y sesión. No hay conexión entre pares entre las computadoras de los asistentes.

Compatibilidad con firewalls

La aplicación para reuniones de WebEx se comunica con Cisco WebEx Cloud para establecer una conexión confiable y altamente segura por HTTPS (puerto 443). Por consiguiente, sus firewalls no necesitan configurarse especialmente para habilitar reuniones de WebEx.

Privacidad de los datos de la reunión

Todo el contenido de las reuniones de WebEx (chat, audio, video, escritorio o documentos compartidos) es transitorio (existe únicamente durante la reunión). El contenido de la reunión no se almacena en una nube de Cisco ni en la computadora de un asistente de manera predeterminada. Cisco conserva solo dos tipos de información de la reunión. Incluyen lo siguiente:

- **Registro de detalles del evento (EDR):** Cisco utiliza los EDR para facturación y generación de informes. Puede consultar información detallada de eventos en su sitio personalizado de WebEx, si inicia sesión con su ID de organizador. Una vez realizada la autenticación, también puede descargar estos datos de su sitio de WebEx o tener acceso a los mismos con diferentes API de WebEx. Los EDR contienen información básica de la asistencia a reuniones, incluido quiénes (nombre de usuario y correo electrónico) se unen a una reunión determinada (ID de la reunión) y cuándo (horas de entrada y salida).
- **Archivos de grabación por red (NBR):** Si un organizador decide grabar una sesión de reunión de WebEx, la grabación se almacena en Cisco WebEx Cloud y queda disponible en el área Mis grabaciones en su sitio personalizado de WebEx. El archivo se creará solo si un organizador habilita NBR durante la reunión o elige una opción para grabar todas las reuniones del sitio. Se puede tener acceso a las NBR a través de enlaces de URL. Cada enlace contiene un token que no puede predecirse. El organizador tiene total control de acceso a un archivo de NBR, incluida la capacidad de eliminarlo, compartirlo o agregar una contraseña para protegerlo. La función de NBR es opcional y el administrador puede desactivarla.

Inicio de sesión único

Cisco admite autenticación federada de usuarios con inicio de sesión único (SSO) que emplea los protocolos de lenguaje de marcado para confirmaciones de seguridad (SAML) 1.1 y 2.0 y WS-Federation 1.0. El uso de SAML 1.1 se está retirando gradualmente. Para usar autenticación federada debe cargar un certificado de clave pública X.509 a su sitio personalizado de WebEx. Después puede generar aserciones SAML que contienen atributos de usuario y firmar digitalmente las aserciones con la clave privada correspondiente. WebEx valida la firma de la aserción SAML según el certificado de clave pública precargado antes de autenticar al usuario.

Informes de terceros

Más allá de sus estrictos procedimientos internos propios, la oficina de seguridad de WebEx involucra a varios terceros independientes para que realicen auditorías rigurosas según las políticas internas, los procedimientos y las aplicaciones de Cisco. Estas auditorías están diseñadas para validar requisitos de seguridad críticos, tanto para aplicaciones comerciales como gubernamentales.

Evaluaciones de seguridad por parte de terceros

Cisco utiliza proveedores externos para realizar pruebas de penetración asistidas por código y evaluaciones de servicio constantes y minuciosas. Parte de la tarea de un proveedor externo comprende realizar las siguientes evaluaciones de seguridad:

- Identificar vulnerabilidades críticas de aplicaciones y servicios, y proponer soluciones
- Recomendar áreas generales para mejora arquitectónica
- Identificar errores de codificación y proporcionar orientación para mejoras en prácticas de codificación
- Trabajar directamente con el personal de ingeniería de WebEx para explicar conclusiones y brindar orientación para acciones correctivas

Certificación Safe Harbor

En marzo de 2012, Cisco obtuvo la Certificación Safe Harbor para los datos de los clientes y partners (la certificación para los datos de los empleados se obtuvo en 2011). Esta certificación sirve como componente adicional al programa integral de cumplimiento de privacidad de Cisco y, si bien no la exige ningún gobierno o consejo de estándares, la empresa reconoce el valor que esta certificación tiene para los clientes.

La Directiva de Protección de Datos de la UE prohíbe la transferencia de datos personales de los ciudadanos europeos a países fuera de la Unión Europea que no cumplan con el estándar de “adecuación” de la UE en términos de protección de la privacidad. El Departamento de Comercio de EE. UU, junto con la Comisión Europea, desarrolló un Marco de Safe Harbor que permite a las organizaciones estadounidenses cumplir con la directiva respetando un conjunto de principios de privacidad de Safe Harbor. Las empresas certifican su cumplimiento de estos principios en el sitio web del Departamento de Comercio de EE. UU. El marco fue aprobado por la UE en el año 2000 y garantiza a las empresas que siguen los principios que la UE considerará sus prácticas como protecciones de privacidad “adecuadas” para los ciudadanos de la UE.

SSAE16

PricewaterhouseCoopers realiza la auditoría anual de Declaración de Normas para Trabajos de Atestificación n.° 16 (SSAE16) de conformidad con estándares establecidos por el Instituto de Contadores Públicos Certificados de los Estados Unidos. Para obtener más información sobre la SSAE16, consulte http://www.ssae16.com.

ISO 27001 y 27002

Cisco logró la certificación ISO 27001 para los servicios de WebEx en octubre de 2012. La certificación se renueva cada tres años con una auditoría externa interina anual. ISO 27001 es un estándar de seguridad de la información publicado por la Organización Internacional de Normalización (ISO) que brinda recomendaciones de mejores prácticas para la creación de un sistema de administración de seguridad de la información (ISMS). Un ISMS es un marco de políticas y procedimientos que incluye todos los controles legales, administrativos, físicos y técnicos involucrados en los procesos de gestión de riesgos de la información de una organización. Según su documentación, ISO 27001 se desarrolló a fin de "ofrecer un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de administración de seguridad de la información". Consulte este enlace para obtener más información sobre ISO 27001 y 27002: http://www.27000.org/.

Más información

Para obtener más información sobre las soluciones de Cisco WebEx visite www.cisco.com/c/es_mx/products/conferencing/index.html o comuníquese con su representante de ventas.

Sede Central en América
Cisco Systems, Inc.
San Jose, 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, los números de teléfono y de fax están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

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