Procedure consigliate Cisco WebEx per riunioni sicure per amministratori di sito e organizzatori

Prima pubblicazione: 15 marzo 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

SOMMARIO

Panoramica della privacy WebEx

Le soluzioni online Cisco WebEx consentono a dipendenti globali e team virtuali di incontrarsi e collaborare in tempo reale come se lavorassero nella stessa sala riunioni. Aziende, istituti ed enti governativi in tutto il mondo si affidano alle soluzioni Cisco WebEx per semplificare i processi aziendali e migliorare i risultati dei team di vendita, marketing, formazione, gestione di progetto e supporto.

Per tutte queste organizzazioni e i relativi utenti, la privacy è di interesse fondamentale. La collaborazione online deve fornire più livelli di sicurezza, dalla pianificazione delle riunioni all'autenticazione dei partecipanti alla condivisione di contenuto.

Cisco WebEx è un ambiente sicuro sebbene possa essere configurato come ambiente aperto di collaborazione. La comprensione delle funzioni di privacy in qualità di amministratori di sito e di utenti finali può consentire la personalizzazione di WebEx in base alle esigenze aziendali.

Per ulteriori informazioni, vedere Whitepaper sulla sicurezza WebEx.

Procedure consigliate per gli amministratori

Una protezione efficace della privacy inizia dall'amministrazione del sito WebEx, che consente agli amministratori di gestire e applicare criteri di privacy per i privilegi di organizzatori e relatori. Ad esempio, un amministratore autorizzato può personalizzare le configurazioni delle sessioni per impedire al relatore di condividere applicazioni o di trasferire file in base al sito o all'utente.

Si consiglia l'uso delle funzioni seguenti per la protezione delle riunioni.

Conversione di tutte le riunioni in riunioni non in elenco

Anche i titoli delle riunioni possono rivelare informazioni sensibili. Ad esempio, una riunione con titolo "Discussione dell'acquisizione della Società A" può avere un impatto finanziario, se rivelata prima del tempo. La creazione di riunioni non in elenco consente di mantenere la privacy delle informazioni sensibili.

Per le riunioni in elenco, l'argomento della riunione e altre informazioni vengono visualizzate sul sito per fare in modo che utenti autenticati, utenti non autenticati e ospiti possano vederli. A meno che la propria organizzazione non abbia un'esigenza aziendale specifica di visualizzare pubblicamente i titoli e le informazioni delle riunioni, tutte le riunioni dovrebbero essere contrassegnate come non in elenco.

Procedura

Passaggio 1 Accedere allo strumento Amministrazione sito WebEx.

Passaggio 2 Andare a **Configurazione > Impostazioni sito comuni > Opzioni > Opzioni di sicurezza**.

Passaggio 3 Selezionare la casella per **Tutte le riunioni non devono essere incluse nell'elenco (MC, TC ed EC)**.

Richiesta di password per tutte le riunioni, eventi e sessioni

Il modo più efficace per garantire la sicurezza di tutte le riunioni, gli eventi e le sessioni di formazione è richiedere una password. Le password proteggono dall'accesso non autorizzato alle riunioni poiché solo gli utenti che conoscono la password possono partecipare. L'applicazione della procedura di richiesta delle password garantisce la sicurezza di tutte le riunioni, gli eventi e le sessioni di formazione create dagli organizzatori.

Si consiglia di utilizzare una password complessa e non facilmente intuibile (password sicura). Una password sicura deve contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (ad esempio, $Tu0psrOx!).

Nota L'aggiunta di password alle riunioni, agli eventi e alle sessioni di formazione non incide sulla partecipazione da parte degli utenti autorizzati. I partecipanti accedono semplicemente selezionando l'URL nell'invito e-mail o dal sito WebEx.

Procedura

Passaggio 1 Accedere allo strumento Amministrazione sito WebEx.

Passaggio 2 Andare a **Configurazione > Impostazioni sito comuni > Opzioni > Opzioni di sicurezza**.

Passaggio 3 Nella sezione Meeting Center, selezionare **Tutte le riunioni devono avere una password**.

Passaggio 4 Nella sezione Event Center, selezionare **Tutti gli eventi devono avere una password**.

Passaggio 5 Nella sezione Training Center, selezionare **Tutti le sessioni devono avere una password**.

Passaggio 6 Per richiedere password sicure, selezionare **Richiedi password complesse per la riunione**.

Passaggio 7 Selezionare e configurare le seguenti caselle:

- Richiesto uso di maiuscole/minuscole
- Lunghezza minima
- Numero minimo di caratteri numerici
- Numero minimo di caratteri alfabetici
- Numero minimo di caratteri speciali
- Non consentire la ripetizione di alcun carattere per più di tre volte
- Non consentire testo di pagine Wb dinamiche per password di riunione (nome sito, nome organizzatore, argomento riunione)
- Non consentire password di riunioni da questo elenco

Applicazione di una password di riunione quando si partecipa da sistemi telefonici o di videoconferenza (WBS30)

Oltre a richiedere le password quando gli utenti accedono da un'applicazione per riunioni (ad esempio, su Windows o Mac), è necessario applicare i requisiti di password agli utenti che accedono da sistemi telefonici o di videoconferenza. Questa funzionalità è disponibile a partire dalla release WBS30. Se questa opzione è selezionata, il sistema genera automaticamente una password numerica di otto cifre per i partecipanti da sistemi telefonici o di videoconferenza e la aggiunge all'invito alla riunione. Ciò assicura che solo le persone con un invito possano accedere alla riunione quando utilizzano un sistema telefonico o di videoconferenza.

Procedura

Passaggio 1 Accedere allo strumento Amministrazione sito WebEx.

Passaggio 2 Andare a **Configurazione > Impostazioni sito comuni > Opzioni > Opzioni di sicurezza**.

Passaggio 3 Nella sezione Meeting Center, selezionare **Applica password riunione in caso di accesso tramite telefono**.

Passaggio 4 Nella sezione Event Center, selezionare **Applica password evento in caso di accesso tramite telefono**.

Passaggio 5 Nella sezione Training Center, selezionare **Applica password sessione di formazione in caso di accesso tramite telefono**.

Passaggio 6 Nella sezione Meeting Center, selezionare **Applica password riunione in caso di accesso tramite sistema di videoconferenza**.

Richiesta di accesso quando si partecipa a una riunione, evento o sessione di formazione (WBS30)

Si consiglia di richiedere a tutti gli utenti di attivare un account sul proprio sito WebEx se vi verranno organizzate riunioni, eventi o sessioni di formazione dal contenuto riservato. Quando questa opzione è abilitata, oltre agli organizzatori, anche ai partecipanti viene richiesto di specificare le proprie credenziali quando tentano di partecipare a una riunione, evento o sessione di formazione.

A partire dalla release WBS30, oltre all'accesso al proprio sito, si consiglia di richiedere l'accesso dei partecipanti che si collegano da un telefono. Ciò impedisce l'accesso alla riunione o alla sessione di formazione a chiunque non sia in possesso delle credenziali appropriate.

Nota I partecipanti che accedono utilizzando l'applicazione Meeting Center o Training Center devono autenticarsi in modo da visualizzare nuovamente la richiesta di autenticazione quando si collegano all'audio. Pertanto, questa limitazione ha impatto solo sugli utenti che partecipano tramite telefono.

Inoltre, si consiglia di limitare la partecipazione da parte di sistemi di videoconferenza a una riunione per la quale è richiesto l'accesso dei partecipanti. Poiché gli utenti non possono accedere da un sistema di videoconferenza, se si consente ai sistemi di videoconferenza di accedere, si rischia l'accesso alla riunione da parte di utenti non autorizzati.

Procedura

Passaggio 1 Accedere allo strumento Amministrazione sito WebEx.

Passaggio 2 Andare a **Configurazione > Impostazioni sito comuni > Opzioni > Opzioni di sicurezza**.

Passaggio 3 Per richiedere che tutti gli utenti dispongano di un account sul sito WebEx per organizzare o partecipare a riunioni, eventi o sessioni di formazione WebEx, selezionare **Richiedi accesso prima di accedere al sito** (solo Meeting Center, Event Center e Training Center).

Passaggio 4 Per richiedere l'accesso quando si partecipa a una riunione o sessione di formazione per telefono, selezionare **Richiedi agli utenti di disporre di un account quando partecipano per telefono** (solo Meeting Center e Training Center).

Se questa opzione è selezionata e l'organizzatore richiede l'accesso, i partecipanti devono accedere dai relativi telefoni. A tale scopo, è necessario che i partecipanti aggiungano un numero di telefono e un PIN alle proprie impostazioni di profilo.

Passaggio 5 Se è richiesto l'accesso per partecipare a una riunione, per evitare ai sistemi di videoconferenza di partecipare, selezionare **Bloccato** (solo Meeting Center).
Se è selezionata l'opzione Bloccato, gli utenti di sistemi di videoconferenza non possono avviare o partecipare alle riunioni che richiedono l'accesso. Ciò include le sale riunioni personali configurate per richiedere l'accesso.

Come disabilitare l'accesso dei partecipanti prima dell'organizzatore

Per tutte le riunioni, non consentire ai partecipanti di accedere prima dell'organizzatore, a meno che non si conosca perfettamente l'impatto di questa scelta sulla sicurezza e tale funzionalità sia effettivamente richiesta.

Si consiglia di disabilitare le opzioni di accesso prima dell'organizzatore per il proprio sito. Si consiglia di disabilitare queste opzioni per le riunioni in elenco, poiché i partecipanti esterni possono utilizzare la riunione pianificata per propri scopi, senza che l'organizzatore ne sia a conoscenza o acconsenta.

In modo analogo, se si consente ai partecipanti di accedere prima dell'organizzatore, si consiglia di impedire loro l'accesso all'audio prima dell'organizzatore. Se la riunione è in elenco sul sito o non è protetta da password, gli utenti non autorizzati potrebbero ottenere potenzialmente l'accesso e avviare chiamate costose senza che l'organizzatore ne sia a conoscenza e acconsenta.

Per le conferenze personali (riunioni PCN), si consiglia di disabilitare l'accesso all'audio prima dell'organizzatore. Un organizzatore deve prima comporre il numero di accesso WebEx per il bridge audio, quindi inserire il codice di accesso organizzatore e il PIN organizzatore prima che i partecipanti possano accedere alla riunione.

Procedura

Passaggio 1 Accedere allo strumento Amministrazione sito WebEx.

Passaggio 2 Andare a **Configurazione > Impostazioni sito comuni > Opzioni > Opzioni di sicurezza**.

Passaggio 3 Per impedire ai partecipanti di accedere prima dell'organizzatore, deselezionare le seguenti caselle:

- **Consenti ai partecipanti o ai coordinatori di partecipare prima dell'organizzatore** (MC, TC e EC)
- **Il primo partecipante a unirsi sarà il relatore** (solo MC)
- **Consenti ai partecipanti o ai coordinatori di partecipare alla teleconferenza prima dell'organizzatore** (MC, TC ed EC)
- **Consenti al partecipante di partecipare alla parte audio della conferenza personale prima dell'organizzatore** (riunioni PCN)

Gestione dell'account

Per gestire le impostazioni dei criteri per tutti gli utenti del sito, le seguenti funzioni sono disponibili anche nel modulo di amministrazione dei sito WebEx:

Gestione dell'account organizzatore

- Bloccare un account dopo un numero configurabile di tentativi di accesso non riusciti

Creazione dell'account

- Richiedere agli utenti di digitare le lettere o le cifre di un'immagine distorta visualizzata sullo schermo
- Richiedere la conferma e-mail dei nuovi account
- Configurare le regole per l'autoregistrazione dei nuovi account

Password account

- Richiedere regole specifiche per il formato, la lunghezza e il riutilizzo delle password
- Consentire la modifica della password a intervalli regolari
- Proibire l'uso di parole facili da intuire (ad esempio, "password")
- Impostare un intervallo di tempo minimo prima della modifica della password

Procedure consigliate per gli organizzatori

In qualità di organizzatore, si ha la responsabilità finale delle impostazioni di sicurezza della propria riunione. Tenere sempre presente che, in qualità di organizzatore, si controllano quasi tutti gli aspetti della riunione, inclusi l'inizio e la fine.

Seguire le procedure consigliate per la sicurezza quando si pianifica la riunione nonché durante e dopo la riunione, in base alle esigenze aziendali, al fine di garantire la sicurezza delle riunioni e delle informazioni.

Uso della sala riunioni personale (WBS30)

Bloccare automaticamente la sala riunioni personale

Con WBS30, è possibile bloccare automaticamente la sala riunioni personale una volta avviata la riunione. A tale scopo, selezionare **WebEx personale >Preferenze > Sala riunioni personale** sul sito WebEx. Si consiglia di bloccare la sala su **0 minuti**. Ciò equivale a bloccare la sala non appena vi si accede. In questo modo, si impedirà a qualsiasi partecipante nell'area di ingresso virtuale di accedere automaticamente alla riunione. Verrà invece visualizzata una notifica nella riunione se sono presenti partecipanti in attesa nell'area di ingresso virtuale. Sarà quindi possibile selezionare i partecipanti e consentire l'accesso alla riunione ai soli partecipanti autorizzati.

Nota Considerare l'URL della sala riunioni personale come un URL pubblico e, a meno che l'amministratore del sito non abbia configurato le sale riunioni personali per l'uso esclusivo da parte degli utenti che hanno eseguito l'accesso, chiunque può attendere nell'area di ingresso virtuale. Controllare sempre i nomi dei partecipanti prima di consentire loro l'accesso alla sala riunioni.

Notifiche delle sale riunioni personali prima di una riunione

Quando gli utenti accedono all'area di ingresso virtuale della sala riunioni personale, possono inviare una notifica e-mail all'organizzatore per indicare che sono in attesa dell'inizio della riunione. Anche gli utenti non autorizzati che ottengono l'accesso all'area di ingresso virtuale della sala riunioni personale possono inviare tali notifiche.

Si consiglia di esaminare le notifiche e-mail prima di avviare una riunione per individuare i partecipanti non autorizzati. Se non è stato impostato il blocco automatico della sala riunioni personale su zero minuti, tutti i partecipanti in attesa nell'area di ingresso virtuale della sala riunioni personale accederanno alla riunione

all'accesso dell'organizzatore. Esaminare l'elenco dei partecipanti ed espellere eventuali partecipanti non autorizzati.

Se è stato impostato il blocco automatico per la sala riunioni personale e si visualizzano troppe notifiche e-mail da partecipanti non autorizzati, disattivare tali notifiche. Andare a **WebEx personale > Preferenze** e disattivare le notifiche della sala riunioni personale deselezionando **Notifica per e-mail quando qualcuno accede all'area di ingresso della mia sala riunioni personale quando sono assente**.

Notifiche delle sale riunioni personali durante una riunione

Se si blocca la sala riunioni personale, è possibile selezionare chi è in attesa nell'area di ingresso virtuale. Una volta eseguito l'accesso alla riunione, ogni volta che un nuovo utente accede all'area di ingresso virtuale si riceve una notifica ed è possibile scegliere se ammettere tale persona o meno. Se nell'area di ingresso virtuale della sala riunioni personale sono presenti più partecipanti, è possibile esaminare l'elenco dei nomi e selezionare i singoli utenti o oppure selezionarli tutti per ammetterli alla riunione.

Pianificazione della riunione

Pianificare le riunioni non in elenco

Per migliorare le impostazioni della privacy della riunione, gli organizzatori possono scegliere di non elencare la riunione nel calendario. A tale scopo, rimuovere il segno di spunta da questa opzione per impedire l'accesso non autorizzato alla riunione e nascondere le informazioni sulla riunione, come organizzatore, argomento e ora di inizio.

- Una riunione non in elenco non viene visualizzata nel calendario delle riunioni nella pagina Sfoglia riunioni o nella pagina Riunioni personali.
- Per partecipare a una riunione non in elenco, il partecipante deve fornire un numero di riunione univoco.
- Le riunioni non in elenco richiedono che l'organizzatore informi i partecipanti alla riunione mediante l'invio di un collegamento in un invito e-mail o che gli organizzatori inseriscano il numero della riunione nella pagina Partecipa a riunioni.

Nota Le riunioni in elenco rivelano i titoli e le informazioni della riunione pubblicamente. Se una riunione non è protetta da password, tutti possono accedervi.

Suggerimento Scegliere un livello di sicurezza in base allo scopo della riunione. Se, ad esempio, si pianifica una riunione per discutere della cena aziendale, probabilmente è necessario specificare solo una password per la riunione. Se, invece, si pianifica una riunione in cui discutere di dati finanziari sensibili, è possibili specificare di non inserire la riunione in alcun elenco. Inoltre, è possibile scegliere anche di limitare l'accesso alla riunione quando tutti i partecipanti si sono uniti a essa.

Scegliere attentamente l'argomento della riunione

Una riunione in elenco o un invito e-mail inoltrato può, come minimo, rivelare il titolo della riunione a persone non desiderate. I titoli delle riunioni possono rivelare accidentalmente informazioni private, pertanto assicurarsi di assegnare titoli che riducano al minimo l'esposizione di dati sensibili, come nomi o eventi della società.

Proteggere la riunione con una password complessa

L'uso di una password complessa per ogni sessione della riunione è il passo più importante nella protezione della riunione. Sebbene non sia una pratica comune, gli amministratori del sito potrebbero scegliere di consentire la creazione di riunioni senza password. In molte circostanze, la protezione di tutte le riunioni con una password sicura è altamente consigliata.

Il passo più importante nell'aumentare la protezione della riunione consiste nella creazione di una password altamente complessa e non facilmente intuibile (password sicura). Una password sicura deve contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (ad esempio, $Tu0psrOx!). Le password proteggono dall'accesso non autorizzato alle riunioni poiché solo gli utenti che conoscono la password potranno partecipare alla riunione.

Non riutilizzare le password per le riunioni. La pianificazione di riunioni con password uguali incide notevolmente sulla protezione della riunione.

Nota L'aggiunta di password alle riunioni non incide sulla partecipazione alla riunione da parte degli utenti autorizzati. I partecipanti possono accedere facilmente a una riunione facendo clic sull'URL nell'invito alla riunione tramite e-mail, applicazione mobile WebEx o altri canali come Cisco Jabber.

Escludere la password della riunione dagli inviti

Se si invitano i partecipanti alla riunione, la password della riunione non appare nei messaggi e-mail di invito ricevuti dai partecipanti. È necessario fornire la password ai partecipanti con un altro mezzo, ad esempio tramite telefono.

Per le riunioni altamente sensibili, escludere la password della riunione dall'invito e-mail. Ciò impedisce l'accesso non autorizzato ai dettagli della riunione qualora il messaggio e-mail di invito venga inoltrato a un destinatario non desiderato.

Richiedere ai partecipanti un account sul sito

Con questa opzione abilitata, tutti i partecipanti devono disporre di un account utente sul sito per partecipare alla riunione. Per ulteriori informazioni su come i partecipanti possono ottenere un account utente, rivolgersi al proprio amministratore di sito.

Nello Strumento di pianificazione anticipata di Meeting Center, selezionare **Richiedi ai partecipanti un account su questo sito Web per unirsi a questa riunione.**

Utilizzare il segnale acustico di entrata o uscita o la funzione di annuncio del nome

L'uso di questa funzione impedisce a una persona di partecipare alla parte audio della riunione senza che l'organizzatore ne sia a conoscenza.

Questa funzione è abilitate per impostazione predefinita per Meeting Center e Training Center. Per regolare le impostazioni, selezionare **Impostazioni conferenza audio > Segnale acustico di entrata e uscita**.

Limitare le funzioni disponibili

Limitare le funzioni disponibili, quali chat e audio, se si consente ai partecipanti di accedere alla riunione prima dell'organizzatore.

Richiedere che gli inviti non vengano inoltrati

Richiedere che gli invitati non inoltrino l'invito, specialmente nel caso di riunioni confidenziali.

Assegnare un organizzatore alternativo

Assegnare un organizzatore alternativo per avviare e controllare la riunione. Ciò consente di garantire maggiormente la sicurezza delle riunioni eliminando la possibilità che il ruolo di organizzatore venga assegnato a un partecipante non previsto o non autorizzato in caso di disconnessione accidentale dalla riunione.

Nota Nell'invitare i partecipanti a una riunione pianificata, è possibile designare uno o più organizzatori alternativi per la riunione. Un organizzatore alternativo può avviare la riunione e agire come organizzatore. Pertanto, un organizzatore alternativo deve disporre di un account utente sul sito Web di Meeting Center.

Durante la riunione

Limitare l'accesso alla riunione

Bloccare la riunione una volta che tutti i partecipanti vi hanno acceduto. Ciò impedirà ad altri partecipanti di accedere alla riunione. Gli organizzatori possono bloccare/sbloccare la riunione in qualsiasi momento mentre è in corso la sessione. Per bloccare una riunione, selezionare **Riunione > Limita accesso**.

Suggerimento Questa opzione impedisce agli altri di partecipare alla riunione, inclusi i partecipanti che sono stati invitati alla riunione ma non si sono ancora uniti. Per sbloccare una riunione, selezionare **Riunione > Ripristina accesso**.

Convalidare l'identità di tutti gli utenti in una chiamata

Verificare la presenza di ogni partecipante mediante un appello è una pratica sicura. Chiedere agli utenti di attivare il video o dichiarare il proprio nome per verificarne l'identità.

Nota

- Per partecipare a una riunione utilizzando un telefono, è sufficiente conoscere un numero di accesso WebEx valido e l'ID riunione di nove cifre. Le password delle riunioni non impediscono ai partecipanti di accedere dalla parte di conferenza audio di WebEx.
- Se si consente ai partecipanti senza un account di accedere alla riunione, gli utenti non autorizzati potranno identificarsi con qualsiasi nome nella riunione.

Rimuovere un partecipante dalla riunione

I partecipanti possono essere espulsi in qualsiasi momento durante una riunione.

Selezionare il nome del partecipante che si desidera rimuovere, quindi selezionare **Partecipante > Espelli**.

Condividere l'applicazione, non lo schermo

Utilizzare **Condividi > Applicazione** anziché **Condividi > Schermo** per condividere applicazioni specifiche e impedire l'esposizione accidentale di informazioni sensibili sullo schermo.

Dopo la riunione

Assegnare password alle registrazioni

Il modo migliore per impedire l'accesso non autorizzato alle registrazioni è non creare le registrazioni.

Se è necessario creare le registrazioni, è possibile modificarle e aggiungere le password prima di condividerle per mantenere la sicurezza delle informazioni. Le registrazioni protette da password richiedono ai destinatari di specificare una password per visualizzarle.

Eliminare le registrazioni

Eliminare le registrazioni non più necessarie.

Servizi di conferenza personale per gli organizzatori

Nella sezione Preferenze WebEx personali del sito WebEx, creare un PIN audio sicuro e proteggerlo.

Il PIN è l'ultimo livello di protezione per impedire l'accesso non autorizzato all'account di conferenza personale. Qualora una persona ottenga accesso non autorizzato al codice di accesso organizzatore per una conferenza personale (riunione PCN), non è possibile avviare la conferenza senza un PIN organizzatore. Proteggere il PIN audio e non condividerlo.