White paper

# Conferenze Web: sfrutta tutte le potenzialità di una collaborazione sicura e in tempo reale

Questo white paper verte sulle informazioni di sicurezza di Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center e Cisco WebEx Event Center.

## Introduzione

Le soluzioni online Cisco WebEx® consentono ai dipendenti e ai team virtuali globali di riunirsi e collaborare in tempo reale, come se si trovassero nella stessa stanza. La collaborazione online offre dei vantaggi aggiuntivi rispetto alla collaborazione diretta tradizionale. Permette infatti di evitare tempi e costi per trasferte e non richiede la disponibilità di ampi spazi per le sale riunioni. Aziende, istituzioni ed enti pubblici di tutto il mondo sfruttano le soluzioni Cisco WebEx® per semplificare i processi aziendali e migliorare i risultati dei team di vendita, marketing, formazione, gestione dei progetti e supporto.

Per tutte queste aziende e organizzazioni, la sicurezza è una priorità fondamentale. La collaborazione online deve garantire la sicurezza a più livelli: dalla pianificazione delle riunioni, all'autenticazione dei partecipanti fino alla condivisione dei documenti.

Per Cisco la sicurezza è una priorità fondamentale nelle fasi di progettazione, distribuzione e gestione della rete, della piattaforma e delle applicazioni. Le soluzioni WebEx® possono essere integrate nei processi aziendali esistenti senza problemi, anche quando i requisiti di sicurezza sono estremamente rigorosi.

È fondamentale comprendere le funzioni di sicurezza delle applicazioni online Cisco WebEx e dell'infrastruttura di comunicazione sottostante (Cisco WebEx Cloud) ai fini delle decisioni di investimento dell'azienda.

## L'infrastruttura Cisco WebEx Cloud

Cisco WebEx Meetings è una soluzione Software-as-a-Service (SaaS), erogata tramite Cisco WebEx Cloud, una piattaforma per l'erogazione di servizi altamente sicura, che garantisce prestazioni, integrazione, flessibilità, scalabilità e sicurezza leader del settore. La facilità di implementazione e distribuzione delle applicazioni che caratterizza Cisco WebEx Cloud permette di ridurre il TCO e assicura al contempo il massimo livello di sicurezza aziendale.

### Architettura di switching

Cisco si avvale di una rete dedicata, distribuita a livello globale, con funzioni di switching ad alta velocità per le riunioni. I dati sulla sessione di una riunione, originati dal computer del relatore e destinati ai computer dei partecipanti, vengono trasmessi, e mai memorizzati in modo permanente, attraverso Cisco WebEx Cloud.[1]

[1] Se l'utente abilita la registrazione di rete (NBR), la riunione viene registrata e memorizzata. Oltre a utilizzare la tecnologia NBR, WebEx memorizza anche i dati relativi ai profili degli utenti, nonché i file degli utenti.

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

### Data center

Cisco WebEx Cloud è un'infrastruttura di comunicazione progettata appositamente per le comunicazioni Web in tempo reale. Le sessioni delle riunioni WebEx sfruttano apparecchiature di switching situate in diversi data center in tutto il mondo. I data center sono posizionati strategicamente vicino ai principali access point Internet e utilizzano una fibra dedicata ad ampia larghezza di banda per instradare il traffico a livello globale. Cisco gestisce l' infrastruttura all'interno di Cisco WebEx Cloud. I dati negli Stati Uniti rimangono nella regione, mentre i dati europei rimangono in Europa.

Inoltre, Cisco utilizza posizioni di rete PoP (Point of Presence) che agevolano l'uso di connessioni backbone, peering Internet, backup globale dei siti e di tecnologie di caching per migliorare le prestazioni e la disponibilità per l'utente finale. I tecnici Cisco sono disponibili 24 ore su 24, sette giorni su sette, per fornire assistenza su sicurezza logistica, operatività e gestione delle modifiche.

## Panoramica sulla sicurezza di WebEx Meetings

WebEx Meetings comprende:

- Configurazione del sito della riunione
- Opzioni di sicurezza per la pianificazione
- Opzioni per l'avvio e la partecipazione a una riunione WebEx
- Tecnologie di crittografia
- Transport Layer Security
- Compatibilità dei firewall
- Privacy dei dati delle riunioni
- Sicurezza dello svolgimento delle riunioni
- Accesso singolo
- Accreditamenti di terze parti (verifiche indipendenti per la convalida della sicurezza di Cisco WebEx)

I termini "riunione/i WebEx" e "sessioni delle riunioni Cisco WebEx" indicano i servizi integrati di conferenza audio, conferenza vocale su Internet e videoconferenza punto a punto e multipunto, utilizzati in tutti i prodotti online Cisco WebEx. Questi prodotti includono:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center (inclusi Cisco WebEx Remote Support e Cisco WebEx Remote Access)

Salvo quanto diversamente indicato, le funzioni di sicurezza descritte nel presente documento sono proprie di tutte le applicazioni e i servizi WebEx sopra elencati.

## Ruoli di WebEx Meetings

Per una riunione WebEx sono previsti quattro ruoli: ospite, ospite alternativo, relatore e partecipante. Nelle sezioni seguenti vengono illustrati i privilegi di sicurezza di ogni ruolo.

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

### Ospite

L'ospite pianifica e avvia la riunione WebEx e controlla l'esperienza dei partecipanti durante la riunione. Dal punto di vista della sicurezza, l'ospite può assegnare il ruolo di relatore ai partecipanti. L'ospite, inoltre, di bloccare la riunione ed espellere i partecipanti.

### Ospite alternativo

L'ospite può nominare un ospite alternativo, che avvia la riunione WebEx pianificata per conto dell'ospite. Dal punto di vista della sicurezza, l'ospite alternativo ha gli stessi privilegi dell'ospite.

### Relatore

Il relatore condivide presentazioni, applicazioni specifiche o l'intero desktop e controlla gli strumenti di annotazione. Dal punto di vista della sicurezza, il relatore può assegnare e revocare il controllo remoto delle applicazioni e del desktop condivisi per singoli partecipanti.

### Partecipante

Il partecipante non dispone di responsabilità o privilegi di sicurezza.

## Modulo WebEx Site Administration

Il modulo WebEx Site Administration consente agli amministratori autorizzati di gestire e applicare policy di sicurezza ai privilegi di ospite e relatore per riunioni specifiche. Ad esempio, è possibile personalizzare le configurazioni delle sessioni per impedire che il relatore possa condividere applicazioni o trasferire file a un sito o a un utente specifico.

Tramite il modulo WebEx Site Administration è possibile gestire le seguenti funzioni di sicurezza:

### Gestione dell'account

- Blocco di un account dopo un numero configurabile di tentativi di accesso falliti
- Sblocco automatico di un account bloccato dopo un determinato intervallo di tempo
- Disattivazione degli account dopo un periodo di inattività definito

### Azioni specifiche dell'account utente

- Richiesta di modifica della password all'accesso successivo
- Blocco o sblocco di un account utente
- Attivazione o disattivazione di un account utente

### Creazione di account

- Richiesta di testo di sicurezza nelle richieste di nuovi account
- Richiesta di conferma tramite e-mail per i nuovi account
- Possibilità di autoregistrazione (iscrizione) per i nuovi account
- Configurazione di regole di autoregistrazione per i nuovi account

### Password dell'account

Applicazione di criteri rigidi per le password degli account, tra cui:

- Maiuscole/minuscole
- Lunghezza minima

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

- Numero minimo di caratteri numerici
- Numero minimo di caratteri alfabetici
- Numero minimo di caratteri speciali
- Impossibilità di ripetizione di un carattere tre o più volte
- Impossibilità di riutilizzo di un numero specificato di password precedenti
- Impossibilità di utilizzo di testo dinamico (nome del sito, nome dell'ospite, nome utente)
- Impossibilità di utilizzo di password incluse in un elenco configurabile (ad esempio, "password")
- Intervallo di tempo minimo prima della modifica della password
- Modifica della password dell'account da parte dell'ospite in un intervallo di tempo configurabile
- Modifica della password dell'account da parte di tutti gli utenti all'accesso successivo

### Sale riunioni personali

Le sale riunioni personali sono accessibili tramite un URL e una password personalizzati. In queste sale l'ospite può elencare le riunioni pianificate e quelle in corso, avviare o partecipare a riunioni e condividere i file con i partecipanti. Gli amministratori possono impostare le funzioni di sicurezza per le sale riunioni personali, tra cui:

- Opzioni per la condivisione di file nella sala riunioni personale
- Requisiti relativi alla password per i file nella sala riunioni personale

## Altre funzioni di sicurezza disponibili nel modulo WebEx Site Administration

- L'ospite o i partecipanti possono scegliere di memorizzare il proprio nome e indirizzo e-mail per semplificare l'organizzazione o la partecipazione alle riunioni successive.
- Gli ospiti possono trasferire la registrazione ad altri ospiti.
- L'accesso al sito può essere limitato tramite la richiesta di autenticazione per l'accesso dell'ospite e di tutti i partecipanti. L'autenticazione può essere richiesta anche per accedere alle informazioni relative al sito, come l'elenco delle riunioni, oltre che per ottenere l'accesso alle riunioni sul sito.
- È possibile applicare regole rigide per le password a WebEx Access Anywhere.
- Tutte le riunioni possono essere rimosse dall'elenco.
- Può essere richiesta l'approvazione per una richiesta di tipo "Password dimenticata?".
- Può essere richiesta la reimpostazione delle password degli account, anziché consentire che vengano inserite nuovamente per conto di un utente.

### Opzioni di sicurezza per la pianificazione delle riunioni WebEx

- È possibile consentire ai singoli ospiti di specificare parametri di sicurezza per l'accesso alle riunioni, che vengono configurati a livello di amministrazione del sito e che non possono essere sovrascritti.
- È possibile rimuovere una riunione dall'elenco in modo che non compaia nel calendario visualizzato.
- È possibile consentire ai partecipanti l'accesso alle riunioni prima dell'acesso dell'ospite.
- È possibile consentire ai partecipanti l'accesso all'audio prima dell'accesso dell'ospite.
- Possono partecipare alla riunione solo i partecipanti dotati di un account del sito WebEx.
- Durante la riunione possono essere visualizzatelLe informazioni sulla teleconferenza.
- Le riunioni possono terminare automaticamente a un'ora stabilita se rimane un solo partecipante.

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

- È possibile richiedere ai partecipanti di inserire il proprio indirizzo e-mail quando accedono alle riunioni.

### Riunioni in elenco o non in elenco

Gli ospiti possono scegliere di elencare una riunione nel calendario riunioni pubblico di un sito WebEx personalizzato. In alternativa, possono pianificare la riunione come "non in elenco", in modo che non compaia nel calendario riunioni. Nel caso delle riunioni "non in elenco", l'ospite deve informare esplicitamente i partecipanti dell'esistenza della riunione attraverso un link inviato via e-mail oppure richiedendo ai partecipanti di inserire il numero della riunione indicato nella pagina di partecipazione alla riunione.

### Riunioni interne o esterne

Gli ospiti possono limitare i partecipanti alla riunione ai titolari di un account sul sito WebEx personalizzato. Tale requisito può essere verificato, in quanto i partecipanti devono accedere al proprio account per partecipare alla riunione.

### Password delle riunioni

L'ospite può impostare una password per la riunione, quindi scegliere di includerla o escluderla nell'e-mail di invito alla riunione.

### Iscrizione

- L'ospite può limitare l'accesso alla riunione tramite la funzione di registrazione. È possibile generare un "elenco di controllo degli accessi" in base al quale viene consentito l'accesso solo agli invitati iscritti ed esplicitamente approvati dall'ospite.
- La sicurezza delle riunioni può essere garantita bloccando il riutilizzo degli ID di registrazione in WebEx Training Center e WebEx Event Center. Ai partecipanti che tentano di riutilizzare un ID di registrazione già in uso verrà impedito di partecipare alla riunione. In questo modo è possibile evitare che gli ID vengano condivisi tra più partecipanti.
- Inoltre, l'ospite può gestire la sicurezza della riunione tramite le limitazioni di accesso e l'espulsione dei partecipanti.

Per supportare le policy di sicurezza aziendali, è possibile impostare qualsiasi combinazione personalizzata delle opzioni di pianificazione disponibili.

### Avvio e partecipazione alla riunione WebEx

La riunione WebEx si avvia previa autenticazione dell'ID utente e della password dell'ospite tramite il sito WebEx personalizzato. L'ospite ha il controllo iniziale della riunione ed è il relatore iniziale, può concedere o revocare permessi di ospite o relatore a qualsiasi partecipante, espellere partecipanti specifici o terminare la sessione in qualsiasi momento.

L'ospite può anche nominare un ospite alternativo per avviare o controllare la riunione nel caso in cui sia impossibilitato a partecipare o perda il collegamento durante la riunione. In questo modo, è possibile intensificare la sicurezza delle riunioni, evitando che il ruolo dell'ospite venga assegnato a un partecipante non previsto o non autorizzato.

Il sito WebEx può essere personalizzato per consentire ai partecipanti di accedere alla riunione, anche per la parte audio, o prima dell'accesso dell'ospite e può limitare le funzioni disponibili per i partecipanti in anticipo unicamente alla chat e all'audio.

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

Quando un partecipante accede per la prima volta a una riunione WebEx, il software client WebEx viene scaricato e installato automaticamente sul suo computer. Il software client WebEx è dotato di firma digitale tramite un certificato emesso da VeriSign. Nelle riunioni successive l'applicazione WebEx scarica e installa solo i file contenenti modifiche o aggiornamenti. Per rimuovere facilmente tutti i file WebEx, i partecipanti possono utilizzare la funzione Disinstalla disponibile nel sistema operativo del computer.

### Tecnologie di crittografia

Le riunioni WebEx sono progettate per fornire contenuti multimediali a tutti i partecipanti in tutta sicurezza e in tempo reale durante una sessione di riunione WebEx. Per consentire a un relatore di condividere un documento o una presentazione, viene utilizzata la tecnologia proprietaria Cisco® UCF (Universal Communications Format) che consente di codificare e ottimizzare i dati per la condivisione. L'applicazione per riunioni WebEx su dispositivi mobili, come iPad, iPhone e BlackBerry, usa meccanismi di crittografia simili al client PC.

Le riunioni WebEx offrono i seguenti meccanismi di crittografia:

- Per le riunioni WebEx su PC e dispositivi mobili, i dati vengono trasmessi dal client a Cisco WebEx Cloud mediante SSL (Secure Sockets Layer) a 128 bit.
- La crittografia end-to-end (E2E) è un'opzione fornita con Cisco WebEx Meeting Center. Questo metodo applica la crittografia end-to-end a tutto il contenuto della riunione tra i partecipanti mediante lo standard AES (Advanced Encryption Standard) con una chiave a 256 bit, generata casualmente sul computer dell'ospite e distribuita ai partecipanti con un meccanismo di chiave pubblica. A differenza della crittografia SSL, che termina sul lato Cisco WebEX Cloud, la crittografia E2E applica la crittografia a tutti i contenuti della riunione nell'infrastruttura Cisco WebEx Cloud. I dati in chiaro, senza crittografia, relativi alla riunione vengono presentati solo nella memoria del computer dei partecipanti.[2]
- Se un utente seleziona l'opzione per la memorizzazione delle credenziali, l'ID di accesso e la password delle riunioni WebEx dell'utente salvati su PC e dispositivi mobili vengono crittografati tramite AES a 128 bit.

Gli amministratori del sito e gli ospiti possono selezionare la crittografia E2E utilizzando l'opzione "Tipo di riunione". La soluzione E2E offre un livello di sicurezza maggiore rispetto al solo AES (sebbene anche la crittografia E2E utilizzi AES per la crittografia del payload), poiché solo l'ospite della riunione e i partecipanti conoscono la chiave.

Ogni connessione dal client WebEx Meeting a WebEx Cloud viene autenticata mediante un token crittografico in modo che solo gli utenti autorizzati possano partecipare a riunioni specifiche.

### Transport Layer Security

Oltre alle protezioni a livello di applicazione, tutti i dati della riunione vengono trasportati tramite SSL a 128 bit. Per attraversare il firewall, anziché usare la porta 80 (usata per il traffico Internet HTTP standard), SSL utilizza la porta 443 del firewall (usata per il traffico HTTPS).

I partecipanti alla riunione WebEx si connettono a Cisco WebEx Cloud con una connessione logica a livello di applicazione, presentazione o sessione. Tra i computer dei partecipanti non si verifica una connessione peer-to-peer.

### Compatibilità dei firewall

L'applicazione WebEx Meetings comunica con Cisco WebEx Cloud per stabilire una connessione sicura e affidabile tramite HTTPS (porta 443). In questo modo, i firewall non necessitano di una configurazione specifica per consentire le riunioni WebEx.

[2] Si noti che NBR non è disponibile quando è abilitata la crittografia E2E. Questa opzione è disponibile solo per WebEx Meeting Center.

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

### Privacy dei dati delle riunioni

Tutti i contenuti delle riunioni WebEx (chat, audio, video, desktop o condivisione di documenti) sono transitori, ovvero esistono solo durante la riunione. Per impostazione predefinita, i contenuti della riunione non vengono memorizzati in cloud Cisco o sul computer dei partecipante. Cisco conserva solo due tipi di informazioni relative alla riunione, ossia:

- **Record dei dettagli dell'evento (EDR):** Cisco utilizza i dati EDR a scopi di fatturazione e report. È possibile rivedere i dettagli dell'evento sul sito WebEx personalizzato accedendo con l'ID dell'ospite. Una volta eseguita l'autenticazione, è altresì possibile scaricare questi dati dal sito WebEx o accedervi attraverso le API di WebEx. Gli EDR contengono informazioni di base sulla partecipazione alle riunioni, tra cui nome utente e indirizzo e-mail dei partecipanti a una riunione specifica (ID riunione), oltre all'ora di inizio e di fine relative alla partecipazione.
- **File della registrazione di rete (NBR):** se un ospite decide di registrare una sessione di WebEx Meetings, la registrazione verrà memorizzata all'interno di Cisco WebEx Cloud e sarà accessibile dall'area delle registrazioni personali del sito WebEx personalizzato. Il file verrà creato solo se un ospite abilita la funzione NBR nel corso della riunione o se sceglie un'opzione applicabile a tutto il sito per registrare tutte le riunioni. È possibile accedere ai file NBR tramite collegamenti URL. Ogni collegamento contiene un token non prevedibile. L'ospite ha il controllo totale sull'accesso a un file NBR, che include anche la possibilità di eliminarlo, condividerlo o aggiungervi una password per proteggerlo. La funzione NBR è facoltativa e può essere disattivata dall'amministratore.

### Accesso singolo

Cisco supporta l'autenticazione federata per l'accesso singolo (SSO) dell'utente tramite SAML (Security Assertion Markup Language) 1.1 e 2.0 e i protocolli WS-Federation 1.0. Il supporto per SAML 1.1 verrà interrotto. L'uso dell'autenticazione federata richiede il caricamento di un certificato a chiave pubblica X.509 sul sito WebEx personalizzato. È quindi possibile generare asserzioni SAML contenenti gli attributi dell'utente e applicare la firma digitale a tali asserzioni con la chiave privata corrispondente. Prima di autenticare l'utente, WebEx convalida la firma di asserzione SAML in base al certificato a chiave pubblica precaricato.

### Report di terze parti

Oltre alle rigide procedure interne, l'Ufficio di sicurezza WebEx coinvolge diverse entità indipendenti di terze parti per condurre controlli rigorosi delle policy, delle procedure e delle applicazioni interne di Cisco. Queste verifiche hanno lo scopo di convalidare i requisiti di sicurezza mission-critical, sia per le applicazioni commerciali che governative.

### Valutazione della sicurezza di terze parti

Cisco si avvale di fornitori di terze parti per eseguire valutazioni dei servizi e test di penetrazione costanti e approfonditi basati sul codice. I fornitori di terze parti coinvolti in tali verifiche eseguono le seguenti valutazioni di sicurezza:

- Identificazione delle vulnerabilità critiche delle applicazioni e/o dei servizi e proposta di soluzioni
- Consigli su aree generali per il miglioramento dell'architettura
- Identificazione degli errori di codifica e assistenza per migliorare le relative pratiche
- Collaborazione diretta con lo staff tecnico di WebEx per illustrare i risultati e offrire assistenza per le azioni correttive

© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.

## Certificazione Safe Harbor

Nel marzo 2012 Cisco ha ottenuto la certificazione Safe Harbor per i dati dei clienti e dei partner (nel 2011 era già stata ottenuta la certificazione Safe Harbor relativa ai dati dei dipendenti). La certificazione rappresenta un ulteriore componente dell'esteso programma Cisco per la conformità alla privacy e, sebbene non sia un requisito obbligatorio per legge, l'azienda riconosce il valore che i clienti attribuiscono a questa certificazione.

La direttiva UE per la protezione dei dati personali vieta il trasferimento dei dati personali dei cittadini europei in paesi extra-europei che non ottemperano agli standard di "adeguatezza" dell'UE in materia di protezione dei dati personali. Il Dipartimento del Commercio degli Stati Uniti, insieme alla Commissione Europea, ha sviluppato il Safe Harbor Framework, che consente alle organizzazioni degli Stati Uniti di conformarsi alla direttiva rispettando una serie di principi sulla privacy Safe Harbor. Le aziende certificano la conformità a tali principi sul sito Web del Dipartimento del Commercio degli Stati Uniti. Il framework è stato approvato dall'UE nel 2000 e offre alle aziende che si attengono a tali principi la garanzia che l'UE considererà le loro procedure in materia di protezione della privacy "adeguate" per i cittadini europei.

### SSAE16

PricewaterhouseCoopers esegue un audit annuale SSAE16 (Statement on Standards for Attestation Engagements No. 16) in conformità agli standard stabiliti dall'organizzazione staunitense American Institute of Certified Public Accountants (AICPA). Per ulteriori informazioni su SSAE16, vedere: http://www.ssae16.com.

### ISO 27001 e 27002

Cisco ha ottenuto la certificazione ISO 27001 per i servizi WebEx nell'ottobre 2012. La certificazione viene rinnovata ogni tre anni con una valutazione intermedia esterna a cadenza annuale. ISO 27001 è uno standard per la sicurezza delle informazioni pubblicato da ISO (International Organization for Standardization) che suggerisce le best-practice per la creazione di un sistema di gestione della sicurezza delle informazioni (ISMS). ISMS è un framework di policy e procedure che includono tutti i controlli legali, amministrativi, fisici e tecnici coinvolti nei processi di gestione del rischio delle informazioni di un'organizzazione. In base alla relativa documentazione, ISO 27001 è stato sviluppato per "fornire un modello per la definizione, l'implementazione, il funzionamento, il monitoraggio, la revisione, la gestione e il miglioramento di un sistema di gestione della sicurezza delle informazioni". Per ulteriori informazioni su ISO 27001 e 27002, visitare: http://www.27000.org/.

## Per ulteriori informazioni

Per ulteriori informazioni sulle soluzioni Cisco WebEx, visitare www.cisco.com/c/it_it/products/conferencing/index.html o contattare il rappresentante di vendita.


**Sede centrale Americhe**
Cisco Systems, Inc.
San Jose, California (USA)

**Sede centrale Asia Pacifica**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Sede centrale Europa**
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e di fax delle sedi italiane sono disponibili nel sito Web Cisco all'indirizzo **www.cisco.com/web/IT/local_offices/contatti_sedi/contatti_sedi_home.html**. Per ottenere maggiori informazioni da Cisco Italia, contattare il numero verde 800 787 854.



Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per visualizzare l'elenco di marchi Cisco, visitare il sito Web all'indirizzo: www.cisco.com/go/trademarks. I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'utilizzo del termine " partner" non implica una relazione di partnership tra Cisco e altre aziende. (1110R)



Stampato negli Stati Uniti C11-709579-01 04/14



© 2014 Cisco e/o i relativi affiliati. Tutti i diritti sono riservati. Il presente documento contiene informazioni pubbliche di Cisco.