Note di rilascio per Cisco Webex Meetings Server Release 4.0

Prima pubblicazione: 2019-04-29

Ultima modifica: 2019-04-29

Note di rilascio per Cisco Webex Meetings Server

Queste note di rilascio descrivono nuove funzioni, requisiti, limitazioni e avvertenze per tutte le versioni di Cisco Webex Meetings Server Release 4.0. Queste note di rilascio vengono aggiornate per ogni rilascio di manutenzione, ma non per patch o aggiornamenti rapidi. Ogni release di manutenzione include funzioni, requisiti, limitazioni e correzioni di bug delle precedenti release, se non indicato diversamente. Prima di distribuire Cisco Webex Meetings Server, si consiglia di rivedere queste note di rilascio per informazioni sui problemi che possono avere effetto sul sistema.

I nuovi clienti possono acquistare Cisco Webex Meetings Server direttamente da Cisco Systems, Inc. o da un rappresentante di vendita del partner.

I clienti esistenti possono ottenere il file OVA della release 4.0 utilizzando lo strumento di aggiornamento del prodotto (PUT): http://upgrad.cloudapps.cisco.com/upgrad/jsp/index.jsp

Per scaricare gli ultimi aggiornamenti software per questo prodotto, visitare: http://software.cisco.com/download.

Selezionare **Prodotti** > **Conferenze** > **Conferenza Web** > **Webex Meetings Server** > **Webex Meetings Server 4.0**.

Ricerca di documentazione

Per la documentazione di amministrazione, visitare: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/tsd-products-support-series-home.html.

Fornire il seguente URL agli utenti: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-user-guide-list.html.

Novità in Cisco Webex Meetings Server Release 4.0

Questa sezione descrive le funzioni nuove o modificate in questa release.

Per un elenco completo dei requisiti di sistema, vedere la *Guida alla pianificazione e requisiti di sistema di Cisco Webex Meetings Server Release 4.0*. Visitare http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Supporto dell'applicazione a 64 bit per Mac

Apple ha annunciato la fine del supporto per le applicazioni a 32 bit; macOS High Sierra sarà l'ultima release macOS a supportare l'architettura a 32 bit. L'applicazione desktop Webex Meetings è un'applicazione a 64 bit.

Supporto di avatar per dispositivi mobili

Gli utenti mobili possono caricare sul sito gli avatar (immagini) da utilizzare nell'applicazione desktop Webex Meetings e nell'app mobile.

I file immagine devono soddisfare i seguenti requisiti:

- Formati di file supportati: PNG, JPG, JPEG e GIF

  Le GIF animate sono supportate, ma il sistema le converte in immagini statiche e utilizza il primo fotogramma come immagine dell'avatar.

- Dimensioni minime dell'immagine: 160 x 160 pixel
- Dimensione massima immagine: 5 MB

Questa funzione richiede l'installazione di storage remoto. Il sistema memorizza gli avatar sul server di amministrazione in /db/archive/avatars/.

Nota I sistemi MDC replicano le immagini degli avatar da un centro dati all'altro.

Supporto del browser

Questa release supporta le seguenti versioni del browser:

Windows:

- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73 e 74
- Microsoft Edge (solo Windows 10): 42.17134.1.0 e 44.17763.1.0
- Microsoft Internet Explorer (IE): 11
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65 e 66

Mac:

- Apple Safari: 12.0.1 (14606.2.104.1.1) e 12.1
- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73 e 74
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65 e 66

Supporto Cisco Jabber

Questa release supporta Cisco Jabber Release 12.1.0, 12.1.1, 12.5.0 e 12.6.0.

Visualizzazione dell'ID chiamante

È possibile abilitare o disabilitare la visualizzazione dell'ID chiamante nel pannello Partecipanti, per gli utenti con chiamata in ingresso. Per attivare o disattivare questa funzione, accedere ad Amministrazione Webex e andare a **Impostazioni** > **Riunioni** > **Impostazioni riunione**. Per impostazione predefinita, questa funzione è disabilitata.

Quando la funzione è disabilitata, l'ID per l'utente con chiamata in ingresso viene visualizzato come: Utente con chiamata in ingresso_N. Esempi:

- Chiamata in ingresso Utente_1
- Chiamata in ingresso Utente_2
- Chiamata in ingresso Utente_3

Quando la funzione è abilitata, l'ID per l'utente con chiamata in ingresso viene visualizzato come: Utente con chiamata in ingresso_N. (<caller ID>). Esempi:

- Utente con chiamata in ingresso_1 (Giacomo Edwards +865516611****)
- Utente con chiamata in ingresso_2 (CHIAMANTE WIRELESS +1650400****)
- Utente con chiamata in ingresso_3 (MARC BROWN +1917929****)

Nota Per motivi di privacy, le ultime quattro cifre sono mascherate da asterischi. È supportata la visualizzazione di massimo 63 caratteri.

Capacità estesa per sistemi MDC

Cisco Webex Meetings Server supporta un sistema di 4000 porte completamente funzionante per i seguenti scenari:

- SDC con alta disponibilità (HA), uso di VMware V-Center 6.5
- MDC- DDC, uso di VMware V-Center 6.5

Sia la capacità estesa sia le funzioni MDC sono disponibili per la release 3.0 ma non sono supportate insieme. Questa release aggiunge il supporto per due sistemi extra large (4000 porte), uniti per creare un MDC. Se si dispone già di un sistema MDC di grandi dimensioni, è possibile estendere entrambi i sistemi per creare un sistema MDC extra large.

La funzionalità di capacità estesa richiede una licenza per ciascun sistema. La licenza di capacità estesa è disponibile solo per sistemi di grandi dimensioni (2000 porte).

Supporto macOS

Questa release supporta le seguenti versioni macOS:

- Sierra 10.12.6
- High Sierra 10.13.6
- Mojave 10.14.1
- Mojave 10.14.2
- Mojave 10.14.3
- Mojave 10.14.4

Vista moderna

Quando gli utenti accedono al sito Webex, possono scegliere tra la vista classica e la vista moderna. Con la vista moderna, possono accedere ai controlli del sito utilizzati più di frequente direttamente da un nuovo

dashboard. Gli utenti possono avviare facilmente le riunioni nella sala riunioni personale Webex, accedere alle riunioni future e pianificare nuove riunioni.

Nella vista moderna, il dashboard è la home page. Gli utenti possono tornare a tale vista in qualsiasi momento selezionando sulla barra di navigazione a sinistra. La vista moderna viene visualizzata per impostazione predefinita, ma è possibile modificare il valore predefinito per il sito Webex.

Sale riunioni personali

Le sale riunioni personali Webex sono spazi per conferenze virtuali sempre disponibili. L'URL della sala riunioni personale e i numeri di chiamata in ingresso rimangono invariati. Gli utenti possono impostare le proprie preferenze per le sale riunioni personali, avviare riunioni immediate e condividere immediatamente i collegamenti per la riunione.

Licenze Smart

Questa release introduce le licenze Smart Software, che semplificano notevolmente tutti gli aspetti della gestione delle licenze. Per ulteriori informazioni sui vantaggi delle licenze Smart Software, vedere le seguenti risorse:

FAQ:https://www.cisco.com/c/dam/en/us/products/collateral/software/smart-accounts/q-and-a-c67-741561.pdf

Informazioni rapide: https://www.cisco.com/c/dam/en/us/products/collateral/ssl-aag.pdf

"Gestione delle licenze" in *Guida all'amministrazione per Cisco Webex Meetings Server*:

https://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

Applicazione desktop Webex Meetings

L'applicazione desktop Webex Meetings sostituisce l'applicazione Webex Meeting e gli Strumenti di produttività. L'applicazione desktop Webex Meetings aggiunge nuove funzioni video e supporto per le sale riunioni personali.

Cisco Webex Meetings Server supporta l'applicazione desktop Webex Meetings versione 39.3.0.582 per Windows e Mac.

Attennzione La pianificazione e la modifica delle riunioni da Microsoft Outlook per Mac non sono supportate. Come soluzione, gli utenti possono pianificare, modificare e avviare riunioni dal sito Webex.

Tabella 1: Funzioni video dell'applicazione desktop Webex Meetings

Funzione	Descrizione
Miniature video	Elenco partecipanti basato su video con miniature video.
Video della vista personale in modalità di condivisione a schermo intero	È possibile visualizzare il video della vista personale sul display principale durante la condivisione in modalità a schermo intero. Avvio o interruzione dell'invio del video dalla finestra del video della vista personale.
Risoluzione ad alta definizione (720p)	Risoluzione video fino a 720p ad alta definizione (1280x720).

Funzione	Descrizione
Blocco video	Il relatore può scegliere quale video verrà visualizzato a tutti i partecipanti.
Trasferimento dell'elaborazione di codifica del video ad alta definizione alla GPU	I chipset GPU supportati possono scaricare l'elaborazione di decodifica dalla CPU dell'host.
Visualizzazione video a schermo intero	Modalità a schermo intero con visualizzazione video ad alta definizione o alta qualità (a seconda della dimensione del monitor) e cinque miniature video.
Visualizzazione video a schermo intero espanso	È possibile espandere la finestra dell'oratore attivo a schermo intero per consentire anche la ricezione di video ad alta definizione.
Collegamento a caldo videocamera	I partecipanti possono collegarsi e scambiare webcam in una riunione.
Regolazione automatica video	Configurazione automatica della qualità video dei partecipanti in base alla larghezza di banda di rete disponibile.
Visualizzazione del video dell'oratore attivo in modalità di condivisione a schermo intero	Visualizzazione del video dell'oratore attivo mobile durante la condivisione a schermo intero.
Trasferimento altoparlante attivo	Trasferimento video automatico ad altoparlante attivo più alto.

Gli aggiornamenti all'applicazione desktop Webex Meetings possono essere resi disponibili sotto forma di patch, release di manutenzione e aggiornamenti rapidi.

Attennzione Se gli utenti si connettono anche ai siti Webex basati su cloud, possono aggiornare l'applicazione desktop Webex Meetings da tali siti. La versione aggiornata funzionerà con Cisco Webex Meetings Server. Il sito a cui l'utente si connette determina l'insieme di funzioni disponibili.

Lettore registrazioni di rete Webex

Questa release supporta le seguenti versioni di Cisco Network Recording Player:

- **Windows:** 39.3.0.582
- **Mac:** 39.3.0.582

Percorsi di potenziamento supportati

Questa release di Cisco Webex Meetings Server supporta i potenziamenti dalla release 1.5 alla 3.0. Si applica quanto segue:

- Per potenziamento si intende la sostituzione del sistema al fine di distribuire modifiche principali apportate al sistema.
- Un aggiornamento è definito come una modifica incrementale del sistema. Gli aggiornamenti apportano correzioni e miglioramenti di entità minore.

- Un aggiornamento conserva tutti i dati del sistema originale. Un potenziamento conserva tutti i dati del sistema originale, tranne i registri.
- Quando si esegue il potenziamento, non è possibile saltare una versione principale del software e passare direttamente a una release di manutenzione (MR).

  Ad esempio, per eseguire un potenziamento dalla versione 1.5MR5 alla versione 3.0MR, eseguire un *potenziamento* dalla versione 1.5MR5 alla versione 3.0, quindi eseguire un *aggiornamento* alla versione 3.0MR.

Nota Tutti gli aggiornamenti richiedono un tempo di inattività. Per i centri MDC, si aggiornano entrambi i centri dati contemporaneamente.

Attenzione Non fare clic su **Riavvia** per un centro dati finché non è completato l'aggiornamento per l'altro ed entrambi visualizzano il pulsante **Riavvia**.

Utilizzare la tabella seguente per determinare il percorso di potenziamento a Cisco Webex Meetings Server Release 4.0.

Dalla release installata…	Percorso per la release 4.0
Da 1.5 a 1.5MR4	**1.** Eseguire l'aggiornamento alla versione 1.5MR5. **2.** Aggiornamento a 1.5MR5 Patch 2 o successiva. **3.** Eseguire il potenziamento alla versione 2.8. **4.** Eseguire l'aggiornamento alla versione 2.8MR1. **5.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **6.** Eseguire il potenziamento alla versione 4.0.
1.5 MR5	**1.** Aggiornamento a 1.5MR5 Patch 2 o successiva. **2.** Eseguire il potenziamento alla versione 2.8. **3.** Eseguire l'aggiornamento alla versione 2.8MR1. **4.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **5.** Eseguire il potenziamento alla versione 4.0.
1.5 MR5 Patch 2 o successiva	**1.** Eseguire il potenziamento alla versione 2.8. **2.** Eseguire l'aggiornamento alla versione 2.8MR1. **3.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **4.** Eseguire il potenziamento alla versione 4.0.

Dalla release installata…	Percorso per la release 4.0
Da 2.0 a 2.0MR8	**1.** Eseguire l'aggiornamento alla versione 2.0MR9. **2.** Eseguire l'aggiornamento alla versione 2.8. **3.** Eseguire l'aggiornamento alla versione 2.8MR1. **4.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **5.** Eseguire il potenziamento alla versione 4.0.
2.0MR9 o versione successiva	**1.** Eseguire l'aggiornamento alla versione 2.8. **2.** Eseguire l'aggiornamento alla versione 2.8MR1. **3.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **4.** Eseguire il potenziamento alla versione 4.0.
Da 2.5 a 2.5MR5	**1.** Eseguire l'aggiornamento alla release 2.5MR6. **2.** Eseguire l'aggiornamento alla versione 2.8. **3.** Eseguire l'aggiornamento alla versione 2.8MR1. **4.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **5.** Eseguire il potenziamento alla versione 4.0.
2.5MR6 o versione successiva	**1.** Eseguire l'aggiornamento alla versione 2.8. **2.** Eseguire l'aggiornamento alla versione 2.8MR1. **3.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **4.** Eseguire il potenziamento alla versione 4.0.
Da 2.6 a 2.6MR2	**1.** Eseguire l'aggiornamento alla versione 2.6MR3. **2.** Eseguire l'aggiornamento alla versione 2.8. **3.** Eseguire l'aggiornamento alla versione 2.8MR1. **4.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **5.** Eseguire il potenziamento alla versione 4.0.
2.6MR3 o versione successiva	**1.** Eseguire l'aggiornamento alla versione 2.8. **2.** Eseguire l'aggiornamento alla versione 2.8MR1. **3.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **4.** Eseguire il potenziamento alla versione 4.0.

Dalla release installata…	Percorso per la release 4.0
2.7 o qualsiasi versione 2.7MR	**1.** Eseguire l'aggiornamento alla versione 2.8. **2.** Eseguire l'aggiornamento alla versione 2.8MR1. **3.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **4.** Eseguire il potenziamento alla versione 4.0.
2.8	**1.** Eseguire l'aggiornamento alla versione 2.8MR1. **2.** Aggiornamento a 2.8MR1 Patch 2 o successiva. **3.** Eseguire il potenziamento alla versione 4.0.
2.8MR1 Patch 2 o successiva	Eseguire il potenziamento alla versione 4.0.
3.0 o qualsiasi versione 3.0MR	Eseguire l'aggiornamento alla versione 4.0.

Importante Non è possibile modificare il tipo di crittografia audio (AE - Audio Encrypted/AU - Audio Unencrypted) per il sistema durante un potenziamento o un aggiornamento. In seguito alla distribuzione, l'unico modo per modificare un sistema da un tipo di crittografia audio all'altro è mediante la distribuzione di un nuovo sistema.

Per ulteriori informazioni, vedere i documenti seguenti:

- *Guida all'amministrazione per Cisco Webex Meetings Server Release 4.0*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Guida all'amministrazione e requisiti di sistema per Cisco Webex Meetings Server Release 4.0*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

Aggiornamento del sistema ad alta disponibilità

Nei sistemi con un sistema ad alta disponibilità (HA) collegato, il sistema HA viene aggiornato automaticamente quando si aggiorna il sistema principale. Assicurarsi che tutte le macchine virtuali HA siano attivate e in esecuzione prima di avviare il processo di aggiornamento.

Per aggiungere un sistema ad alta disponibilità (HA) al sistema principale, distribuire prima il sistema HA. Successivamente, aggiornare il sistema HA alla stessa versione del sistema principale. Il sistema HA si riavvia alla fine del processo di aggiornamento. Si consiglia di attendere altri 15 minuti dopo il riavvio prima di iniziare ad aggiungere il sistema HA al sistema principale.

Per ulteriori informazioni, vedere *Guida all'amministrazione di Cisco Webex Meetings Server* per la release in uso:

http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

Limitazioni e restrizioni

Riunioni solo audio

Nelle seguenti circostanze, una riunione può continuare oltre la durata massima della riunione di 24 ore:

- Tutti i partecipanti a una riunione Webex normale sono con chiamata in ingresso (solo audio).
- Nessun partecipante avvia la parte Web della riunione.

In questo caso, la riunione continua fino a quando un partecipante rimane nella conferenza. Se tutti i partecipanti con chiamata in ingresso si disconnettono dalla conferenza, la riunione termina entro 24 ore dall'ora di inizio. La riunione termina immediatamente se si protrae oltre l'ora di fine pianificata.

Nota Questo scenario si applica solo alle riunioni Webex normali a cui accedono solo partecipanti con chiamata in ingresso. Questo scenario non si applica alle riunioni con numero di conferenza personale (PCN) o alle riunioni Webex normali a cui accedono partecipanti Web.

Rimozione del proxy inverso Internet

Come parte del processo di rimozione del nodo del proxy inverso Internet (IRP), la macchina virtuale di amministrazione invia un messaggio di rimozione al server IRP. Il messaggio rimuove il server IRP e pertanto impedisce tutti gli accessi esterni al sistema. Il messaggio viene inviato come testo normale e senza autenticazione. Codice dannoso appositamente prodotto potrebbe replicare questo funzionamento e provocare un Denial of Service.

Si consiglia di limitare l'accesso alla porta 64616, sul nodo IRP, alla sola macchina virtuale di amministrazione.

Limitazioni di registrazione

La dimensione massima di ogni registrazione è 2.2 GB (limite di sistema esistente). Per i centri MDC, assicurarsi che esista capacità di storage sufficiente per tutti i centri dati. Il numero massimo di registrazioni dipende dalla capacità del server di storage. È possibile stimare la dimensione del server di storage richiesta per un periodo tipico di cinque anni utilizzando la formula seguente:

Ore stimate di riunioni che si prevede di registrare al giorno * 50-100 MB per ora di registrazione * cinque anni * 24 ore al giorno * 365 giorni all'anno

Non è prevista alcuna limitazione di storage per utente. Il sistema memorizza le registrazioni a tempo indefinito finché gli utenti non le eliminano. Per evitare l'eliminazione accidentale di registrazioni importanti, non è presente alcuna impostazione che abiliti l'eliminazione automatica delle registrazioni. Il server di storage conserva le registrazioni contrassegnate per l'eliminazione per un periodo di sei mesi. Durante tale tempo, gli utenti possono comunque archiviare le registrazioni su altri supporti.

Quando si configura un server di storage e si seleziona **Registra** in **Dashboard di amministrazione** > **Impostazioni** > **Riunioni** > **Privilegi partecipante**, l'impostazione **Registra** è un'impostazione a livello di sistema. Per le registrazioni non esistono impostazioni o preferenze per le singole riunioni. È anche possibile abilitare o disabilitare la registrazione per tipi di sessione, assegnati agli utenti.

Tipi di sessione

Un tipo di sessione è un pacchetto predefinito di funzioni e opzioni (profilo) che gli amministratori di sito possono personalizzare e assegnare agli utenti. Il tipo di sessione predefinita (riunione) è il tipo di sessione

PRO. A causa delle relazioni tra il tipo di sessione PRO e i tipi di sessione personalizzati, si consiglia di non modificare il tipo di sessione PRO. La procedura ottimale consiste nel creare un tipo di sessione personalizzato da modificare.

Modifiche SSO e agli indirizzi e-mail

Con questa release, il server provider di identità (IdP) può utilizzare qualsiasi campo Active Directory (AD) univoco e statico come NameID per la configurazione SSO. Se si intende utilizzare la funzione di modifica dell'indirizzo e-mail, il campo AD e-mail non è statico. Modificare l'associazione per il campo NameID sul server IdP in un campo AD univoco diverso dall'e-mail. Se non si intende utilizzare la funzione per la modifica degli indirizzi e-mail, non è necessario modificare l'associazione per il campo NameID.

Attenzione Se il campo NameID viene associato al campo AD e-mail e si modificano gli indirizzi e-mail degli utenti, il sistema crea un nuovo account utente per ciascun indirizzo modificato.

Se si intende modificare l'associazione del campo NameID dall'e-mail a un altro campo (come EmployeeNumber), gli utenti devono prepararsi alla modifica. Dopo aver aggiornato i campi NameID in AD, fare in modo che gli utenti accedano a CWSM prima di modificare gli indirizzi e-mail. In caso contrario, quando entrambi gli indirizzi NameID ed e-mail cambiano, nessun attributo corrisponde al profilo CWMS. In questo scenario, il profilo esistente perde la possibilità di accedere al sistema e il sistema crea un nuovo profilo.

Outlook si sincronizza con il server Exchange una volta al giorno. Se si modifica l'indirizzo e-mail di un utente esistente sul server Exchange, tale modifica non viene propagata immediatamente ad Outlook. Finché non viene eseguita la sincronizzazione, il sistema riceve l'indirizzo e-mail precedente dell'utente ed emette un avviso che l'utente non è stato trovato. Un utente delegato (proxy) non può pianificare una riunione per l'utente o nominarlo come organizzatore alternativo finché Outlook non esegue la sincronizzazione con il server Exchange.

La sincronizzazione manuale del sistema non risolve questo problema. Questa limitazione non è un problema CWMS, ma è dovuto al funzionamento di Outlook ed Exchange.

*Vedere anche*Informazioni sulla configurazione SSO, a pagina 13.

Browser Microsoft Edge

Il browser Microsoft Edge non supporta la riproduzione delle registrazioni Webex.

Supporto vCenter 6.5

Quando si distribuisce il file OVA di CWMS su vCenter 6.5, si applicano le seguenti restrizioni:

- A causa delle limitazioni del browser e della dimensione del file OVA di CWMS pari a 16 GB, è necessario distribuire il file OVA utilizzando l'URL e non il file locale aggiornato.
- Scegliere il file basato su FLASH vCenter. Questa selezione è necessaria per inserire correttamente le proprietà vApp per la configurazione VM: nome host, dominio, indirizzo IP, subnet e configurazione DNS.

Infrastruttura desktop virtuale

Di seguito sono riportate le limitazioni note che incidono sugli ambienti con infrastruttura desktop virtuale (VDI).

- Citrix Virtual Apps and Desktops è il solo software di virtualizzazione software supportato per questa release di Cisco Webex Meetings Server.
- Una limitazione architetturale dell'ambiente con desktop virtuale può avere un effetto sulla qualità video. La velocità di riproduzione potrebbe essere lenta provocando prestazioni non ottimali nell'invio di video.
- Alcuni file video non possono essere condivisi in un ambiente desktop virtuale.
- Remote Access e Access Anywhere non sono supportati negli ambienti con desktop virtuale. La piattaforma Citrix sottostante rimuove gli agenti Remote Access ed Access Anywhere dopo il riavvio del sistema operativo.

Applicazione desktop Webex Meetings

L'applicazione desktop Webex Meetings presenta le seguenti limitazioni. Gli utenti non possono eseguire le seguenti azioni:

- Pianificare una riunione annuale.
- Accesso a una riunione con un indirizzo video.
- Pianificazione o accesso alle riunioni nella sala riunioni personale dall'applicazione desktop Webex Meetings.
- Pianificazione di riunioni nella sala riunioni personale da Microsoft Outlook.
- Connessione e accesso alle riunioni da dispositivi video.
- Connessione e condivisione con dispositivi video registrati su cloud.
- Connessione e condivisione con dispositivi Webex Share.
- Ricezione di una richiamata su un dispositivo video durante una riunione (Chiama sistema video personale).
- Avvio o accesso a una riunione da Microsoft Word, PowerPoint o Excel.

Attennzione La pianificazione e la modifica delle riunioni da Microsoft Outlook per Mac non sono supportate. Come soluzione, gli utenti possono pianificare, modificare e avviare riunioni dal sito Webex.

Considerazioni sull'aggiornamento

L'applicazione desktop Webex Meetings non è compatibile con le versioni precedenti di Cisco Webex Meetings Server.

Dopo aver aggiornato il sistema a CWMS 4.0, è possibile scegliere se eseguire il push dell'applicazione agli utenti finali o consentire loro di scaricarla da soli.

Se si esegue il push dell'applicazione desktop Webex Meetings agli utenti, questi ultimi devono accedere all'applicazione con le credenziali esistenti. Ciò è vero, anche se in precedenza hanno scelto le opzioni di memorizzazione utente e accesso automatico per gli Strumenti di produttività Webex.

Se si consente agli utenti di scaricare e installare l'applicazione da sé, gli utenti Microsoft Windows devono prima disinstallare gli Strumenti di produttività Webex.

Se consentito, alcuni utenti possono scegliere di continuare a utilizzare gli Strumenti di produttività Webex. Questi utenti non saranno in grado di avviare riunioni immediate facendo clic sul pulsante **Avvia riunione**. È disponibile un aggiornamento rapido per risolvere questo problema.

Note importanti

Supporto Hypervisor

Cisco Webex Meetings Server viene eseguito su macchine virtuali VMware.

- Entrambi VMware vSphere e VMware vCenter sono necessari per distribuire Cisco Webex Meetings Server. Utilizzando il client vSphere, si distribuisce il file OVA di Cisco Webex Meetings Server su un host ESXi gestito da vCenter.
- Acquistare VMware vSphere 5.5, 6.0 o 6.5 per utilizzarlo come piattaforma hypervisor per Cisco Webex Meetings Server.
  - Acquistare vSphere direttamente da Cisco su GPL (Global Price List). Cisco è un partner e distributore approvato VMware. Questa soluzione è particolarmente conveniente per coloro che desiderano acquistare tutto da un unico fornitore.
  - Acquistare vSphere direttamente da VMware, attraverso i contratti aziendali diretti con VMware.
- Cisco Webex Meetings Server non supporta altri hypervisor.
- Per ulteriori informazioni sui requisiti hypervisor, vedere la *Guida alla pianificazione e requisiti di sistema per Cisco Webex Meetings server* su http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Informazioni sull'uso di certificati autofirmati

Si consiglia di utilizzare un certificato firmato pubblicamente anziché fornire un certificato autofirmato. I browser degli utenti considerano attendibili i certificati firmati pubblicamente poiché l'elenco dei certificati dell'autorità di certificazione principale installati sul computer ne stabilisce l'attendibilità.

Per sistemi MDC che utilizzano certificati autofirmati, l'utente finale riceve più avvisi sui certificati e deve identificare come affidabili e installare tutti i certificati per utilizzare il sistema.

Quando si utilizzano certificati autofirmati, alcuni utenti possono avere difficoltà a partecipare alle riunioni, in quanto i browser per impostazione predefinita non riconoscono tali certificati come attendibili. Gli utenti devono, in questo caso, stabilire in modo esplicito la relazione di trust prima di partecipare a una riunione sul sito. Alcuni utenti potrebbero non comprendere come stabilire una relazione di trust con un certificato. Altri potrebbero non essere autorizzati a eseguire questa operazione in base alle impostazioni dell'amministratore. Utilizzare certificati firmati pubblicamente, ove possibile, per offrire la migliore esperienza agli utenti.

La Guida utente fornisce più informazioni su questo problema per gli utenti. Vedere l'argomento «Il client per riunioni non viene caricato» nel capitolo «Risoluzione dei problemi» della *Guida utente di Cisco Webex Meetings Server* su http://www.cisco.com/en/us/products/ps12732/products_user_guide_list.html.

Tipi di crittografia supportati

Cisco Webex Meetings Server supporta i seguenti tipi di crittografia:

TLS versione 1.1

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)

TLS versione 1.2

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)

Supporto TLS

Questa release supporta TLS 1.1 e versioni successive; TLS 1.0 non è supportato, con un'eccezione. Sono supportate le connessioni client da Cisco Webex Meetings Server (CWMS) a un server SMTP tramite TLS 1.0.

Questa release supporta Cisco Unified Call Manager (CUCM) 8.6 o 9.0 senza TLS/SRTP e CUCM 9.1, 10.0, 10.5, 11.0(1a), 11.5(1)SU1, 11.5(1)SU3 e 12.0 per la teleconferenza sicura.

Informazioni sulla configurazione SSO

Questa release supporta l'uso di qualsiasi campo Active Directory (AD) come NameID per la configurazione SSO. Si consiglia di utilizzare i seguenti attributi AD per la configurazione di NameID per SSO:

- E-mail
- SAMAccountName
- UserPrincipalName (UPN)
- Numero di telefono
- EmployeeNumber
- ObjectSid

Attributi di asserzione SAML obbligatori

I seguenti attributi di asserzione SAML sono richiesti per la funzioni di creazione automatica dell'account:

- Cognome
- FirstName
- e-mail

Importante L'attributo e-mail è sempre richiesto anche se la creazione automatica dell'account e l'aggiornamento automatico dell'account sono disabilitati nella configurazione SSO.

Espansione del sistema

Se si dispone di snapshot VMware sul sistema esistente (pre-espansione), rimuoverle prima di iniziare l'espansione.

L'espansione del sistema richiede il collegamento del disco della macchina virtuale (VMDK) dal sistema originale al sistema di destinazione (espanso). Se si lasciano gli snapshot sul sistema originale e si collega quest'ultimo al sistema di destinazione, il sistema di destinazione non si accende a causa dell'incoerenza di snapshot.

Nomi comunità SNMP v2

Non esiste alcun nome di comunità SNMP v2 predefinito in questa release di Cisco Webex Meetings Server. Il nome di comunità predefinito Cisco Webex Meetings Server 1.0 esistente, "CWS-Public", verrà rimosso dopo l'aggiornamento. Solo i nomi di comunità SNMP v2 aggiunti da utenti vengono conservati.

Documentazione tradotta

La documentazione tradotta per questa release di Cisco Webex Meetings Server viene pubblicata 4–6 settimane dopo il rilascio della versione inglese.

Problemi noti e avvisi

Apple iOS 6.x e SSO

Esiste un problema noto con Apple iOS 6.x. Il Single Sign-On (SSO) non funziona per gli utenti interni di iPad/iPhone che utilizzano il browser Web Safari 6. Questo problema era provocato da un difetto di Apple, corretto in iOS 7. L'ID del bug Safari è 13484525.

Configurazione audio

Nelle impostazioni di configurazione audio, G.711 fornisce una migliore qualità vocale rispetto a G.729. Per ulteriori informazioni, vedere «Informazioni sulla configurazione delle impostazioni audio» nella *Guida all'amministrazione di Cisco Webex Meetings Server*.

Impossibile condividere file video in formato .mp4 su Windows

Quando si utilizza QuickTime, viene visualizzato il seguente messaggio: «QuickTime non inizializzato. N. errore –2093. Accertarsi che QuickTime sia installato correttamente su questo computer.»

Questo messaggio di errore può indicare che il file QuickTime.qts è mancante, è stato spostato o non è utilizzabile. Il file QuickTime.qts si trova nella directory \WINDOWS\SYSTEM. Per risolvere questo sintomo, rimuovere completamente e reinstallare QuickTime.

1. Scaricare l'ultima versione di QuickTime Player http://www.apple.com/quicktime/download/.
2. Disinstallare QuickTime utilizzando l'opzione **Installazione applicazioni** nel pannello di controllo. Assicurarsi di selezionare **Disinstalla tutto**.

3. Eliminare il contenuto della cartella Temp, C:\WINDOWS\TEMP (se esistente).
4. Installare QuickTime utilizzando la versione di QuickTime scaricata.
5. Riavviare Windows.

Problema del dashboard nella visualizzazione delle riunioni avviate

In questa release di Cisco Webex Meetings Server, il dashboard talvolta non riesce a visualizzare alcune riunioni come avviate. Questo problema si verifica nel seguente scenario:

Una riunione è pianificata con l'impostazione **Consenti ai partecipanti di unirsi alla teleconferenza prima dell'organizzatore** abilitata. Un partecipante si unisce alla riunione per telefono, ma non partecipa alla parte Web. Il dashboard dovrebbe indicare che questa riunione è stata avviata e che è presente un partecipante, ma ciò non accade. In questo caso, gli utenti potrebbero pianificare più riunioni, con un impatto sulle prestazioni.

Connessioni di chiamata in ingresso e chiamata in uscita per una riunione in corso

In caso di failover di una riunione da un centro dati a un altro, le connessioni con chiamata in entrata e in uscita a tale riunione non vengono ristabilite automaticamente. Per ristabilire le connessioni, i partecipanti agganciano e richiamano manualmente per accedere.

Questo problema può verificarsi quando:

- Il sistema installato e un MDC grande.
- La riunione viene avviata mentre uno dei centri dati è in Modalità di manutenzione o è spento.
- Quando, dopo aver disattivato la Modalità di manutenzione o aver acceso il centro dati, un altro centro dati viene spento o messo in Modalità di manutenzione.

Endpoint IP Communicator 7.0.x

Gli endpoint IP Communicator 7.0.x che accedono alle riunioni CWMS possono introdurre problemi di qualità (echi e altri disturbi) a una conferenza, se si verifica una delle seguenti condizioni:

- L'audio di IP Communicator non viene disattivato.
- Un partecipante che utilizza IP Communicator diventa l'oratore attivo.

Per evitare questo problema, impostare in modo preciso l'ambiente IP Communicator (ad esempio, cuffia, microfono e altoparlante) o utilizzare un altro telefono tradizionale.

Uso dello stesso nome host quando si modifica l'indirizzo IP della macchina virtuale

Non modificare mai le voci DNS per i nomi host configurati nella distribuzione. È possibile modificare il nome host di una macchina virtuale che fa parte della distribuzione. L'indirizzo IP corrispondente viene selezionato automaticamente dal DNS. Se si desidera modificare l'indirizzo IP di una macchina virtuale e mantenere lo stesso nome host, è necessario effettuare le seguenti operazioni:

1. Configurare un nome host temporaneo nel DNS.
2. Modificare il nome host della macchina virtuale nel nome host temporaneo configurato.
3. Disattivare la modalità di manutenzione per il sistema per rendere effettiva la modifica del nuovo nome host.

   I nomi host originali non fanno parte della distribuzione dopo questa modifica.

4. Modificare l'indirizzo IP del nome host originale nel DNS nel nuovo indirizzo IP.
5. Modificare il nome host temporaneo della macchina virtuale nel nome host originale.
6. Disattivare la modalità di manutenzione per il sistema per rendere effettiva la modifica del nome host.

   A questo punto, il nome host originale è configurato con il nuovo indirizzo IP.

Aggiornamento dalla release 3.0 patch 1 non riuscito

L'aggiornamento dalla release 3.0 patch 1 (3.0.1.33) non riesce poiché sono presenti dati errati nel file cwms.pub. Prima di eseguire l'aggiornamento dalla release 3.0 patch 1, applicare la seguente soluzione per questo problema.

1. Passare a https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj70890.
2. Scaricare il file allegato: `fix_update.zip` e copiarlo nella directory `/archive` della VM di amministrazione principale.
3. Utilizzare SSH per connettersi alla VM di amministrazione principale e passare alla directory `/archive`.
4. Decomprimere il file: **unzip fix_update.zip**.
5. Rendere eseguibile il file decompresso: **chmod +x fix_update**.
6. Eseguire l'eseguibile: **./fix_update**.
7. Dopo aver visualizzato il messaggio `Operazione riuscita`, procedere con l'aggiornamento.

Avvertenze

Uso dello strumento di ricerca dei bug

Problemi noti (bug) vengono classificati in base al livello di gravità. Queste note di rilascio contengono una descrizione dei seguenti elementi:

- Bug aperti riscontrati dai clienti di severità 1 - 3
- Bug risolti riscontrati dai clienti di severità 1 - 3
- Bug risolti rilevati da Cisco di una certa importanza

Per ottenere dettagli sui bug elencati e per ricercare altri bug, è possibile utilizzare lo Strumento di ricerca dei bug.

Prima di iniziare

Per accedere allo Strumento di ricerca dei bug, occorre quanto segue:

- Connessione Internet
- Browser Web
- ID utente e password Cisco.com

Procedura

Passaggio 1 Per accedere allo Strumento di ricerca dei bug, andare a https://tools.cisco.com/bugsearch/search.

Passaggio 2 Eseguire l'accesso utilizzando ID utente e password Cisco.com.

Passaggio 3 Immettere il numero ID del bug nel campo "Cerca" e premere **Invio**.

Suggerimento È possibile passare a un bug specifico inserendo dove è l'ID del bug che si sta ricercando (ad esempio, CSCab12345).https://tools.cisco.com/bugsearch/bug/<BUGID><BUGID>

Operazioni successive

Per informazioni su come ricercare i bug, creare ricerche salvate e gruppi di bug, selezionare **Guida** nella pagina **Strumento di ricerca dei bug**.

Avvertenze chiuse per Cisco Webex Meetings Server Release 4.0

La tabella seguente elenca le avvertenze (bug) chiuse per questa release.

Tabella 2: Avvertenze chiuse per Cisco Webex Meetings Server Release 4.0 (Build 4.0.1.19)

ID avvertenza	Gravità	Titolo
CSCvp08700	3	Win: Gli Strumenti di produttività precedenti non possono aggiornare/eliminare le riunioni pianificate dalla nuova app Webex.
CSCvm99626	4	Certificato intermedio perso dopo l'aggiornamento a 2.8 MR2 o 3.0 MR2

Avvertenze aperte per Cisco Webex Meetings Server Release 4.0

La tabella seguente elenca le avvertenze (bug) aperte per questa release.

Tabella 3: Avvertenze aperte per Cisco Webex Meetings Server Release 4.0 (Build 4.0.1.19)

ID avvertenza	Gravità	Titolo
CSCvp34644	2	Arresto anomalo della riunione T39 durante la condivisione
CSCvp30778	3	L'app desktop non è riuscita ad avviare la riunione Webex senza messaggi di errore
CSCvo98359	3	PT precedenti: L'avvio della riunione immediata non riesce dagli Strumenti di produttività precedenti quando si accede al sito 4.0.
CSCvp32096	3	Il partecipante non riceve il messaggio e-mail relativo alla disponibilità della registrazione

Avvertenze risolte per Cisco Webex Meetings Server Release 4.0

La tabella seguente elenca le avvertenze (bug) aperte in una release precedente e chiuse per questa release.

Tabella 4: Avvertenze risolte per Cisco Webex Meetings Server Release 4.0 (Build 4.0.1.19)

ID avvertenza	Gravità	Titolo
CSCvj02258	3	Aggiornamento automatico alla release 3.0 non riuscito dal sistema con HA
CSCvn47005	3	Giorni di fine settimana del calendario errati
CSCvn67024	3	Impossibile accedere a PT quando l'Editore CUCM è inattivo e l'integrazione della rubrica è passata a CUCM Sub
CSCvp16492	3	Quando viene trasferita una chiamata dall'endpoint SRTP all'endpoint RTP, non è presente alcun audio
CSCvo56983	3	Gli utenti non vengono inseriti nella casella di ricerca dalla pagina di amministrazione né dal campo WHO dall'impostazione della riunione Web
CSCvp03915	3	La password utente USM SNMP non può contenere il segno "$"
CSCvn77979	4	L'opzione Imponi a tutti gli utenti la modifica della password ogni [x] giorni incide anche sugli utenti LDAP
CSCvo51406	4	I numeri di richiamata non vengono visualizzati nel browser Edge
CSCvo12211	4	Il numero di partecipanti nei risultati della ricerca della riunione non riportano valori esatti

Ulteriori informazioni e richieste di assistenza

Per informazioni sull'invio di una richiesta di assistenza e per ulteriori informazioni, andare a http://www.cisco.com/c/en/us/support/index.html.

È anche possibile eseguire l'iscrizione ai feed RSS di Cisco Security e ricevere notifiche quando sono disponibili nuove informazioni. I feed di contenuto sono disponibili in entrambe le versioni 1.0 e 2.0 del formato RSS. Visitare http://tools.cisco.com/security/center/rss.x?i=44.