Guida all'amministrazione del telefono IP Cisco serie 8800 per Cisco Unified Communications Manager

Prima pubblicazione: 2015-07-13

Ultima modifica: 2023-06-16

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

LE SPECIFICHE E LE INFORMAZIONI SUI PRODOTTI RIPORTATE DEL PRESENTE MANUALE SONO SOGGETTE A MODIFICHE SENZA PREAVVISO. TUTTE LE DICHIARAZIONI, INFORMAZIONI E RACCOMANDAZIONI CONTENUTE NEL PRESENTE MANUALE SONO DA CONSIDERARSI ACCURATE MA VENGONO FORNITE SENZA ALCUN TIPO DI GARANZIA, ESPLICITA O IMPLICITA. GLI UTENTI DEVONO ASSUMERSI LA PIENA RESPONSABILITÀ PER L'UTILIZZO DI QUALSIASI PRODOTTO.

LA LICENZA SOFTWARE E LA GARANZIA LIMITATA PER IL PRODOTTO VENGONO DEFINITE NEL PACCHETTO INFORMATIVO FORNITO CON IL PRODOTTO E SONO IVI INCLUSE TRAMITE QUESTO RIFERIMENTO. IN CASO DI DIFFICOLTÀ A INDIVIDUARE LA LICENZA O LA GARANZIA LIMITATA DEL SOFTWARE, RICHIEDERNE UNA COPIA AL RAPPRESENTANTE CISCO DI RIFERIMENTO.

Le informazioni riportate di seguito si riferiscono alla conformità FCC dei dispositivi di classe A: la presente apparecchiatura è stata collaudata ed è risultata conforme ai limiti stabiliti per un dispositivo digitale di Classe A, ai sensi della Parte 15 delle regole FCC. Tali limiti sono studiati per garantire un grado di protezione sufficiente contro le interferenze dannose quando l'apparecchiatura viene utilizzata in ambienti commerciali. La presente attrezzatura genera, utilizza e può emettere frequenze radio e, se non installata e utilizzata secondo il manuale di istruzioni, può causare interferenze dannose per le comunicazioni radio. È probabile che l'utilizzo dell'apparecchiatura in aree residenziali determini interferenze dannose. In tal caso, gli utenti dovranno porre rimedio a proprie spese.

Le informazioni riportate di seguito si riferiscono alla conformità FCC dei dispositivi di classe B: la presente apparecchiatura è stata collaudata ed è risultata conforme ai limiti stabiliti per un dispositivo digitale di Classe B, ai sensi della Parte 15 delle regole FCC. Tali limiti sono stati stabiliti con lo scopo di fornire adeguata protezione da interferenze dannose in installazioni di tipo residenziale. La presente attrezzatura genera, utilizza e può emettere frequenze radio e, se non installata e utilizzata secondo le istruzioni fornite, può causare interferenze dannose per le comunicazioni radio. Tuttavia, non si fornisce alcuna garanzia che tali interferenze non si verifichino in particolari condizioni di installazione. Se accendendo e spegnendo l'apparecchiatura si rilevasse che questa provoca interferenze dannose alla ricezione radio-televisiva, si consiglia di correggere l'interferenza adottando una delle seguenti misure:

- Riorientare o riposizionare l'antenna di ricezione.
- Aumentare la distanza tra l'apparecchiatura e il ricevitore.
- Collegare l'apparecchiatura a una presa diversa da quella del ricevitore.
- Chiedendo assistenza al rivenditore o a un tecnico esperto in impianti radiotelevisivi.

Eventuali modifiche apportate al prodotto senza l'autorizzazione di Cisco possono comportare la perdita di validità dell'approvazione FCC e l'annullamento del diritto a utilizzare l'apparecchiatura.

L’implementazione Cisco della compressione delle intestazioni TCP è un adattamento di un programma sviluppato dalla University of California (UCB) di Berkeley nell'ambito della sua versione disponibile al pubblico del sistema operativo UNIX. Tutti i diritti riservati. Copyright © 1981, Regents of the University of California.

NONOSTANTE EVENTUALI ALTRE GARANZIE FORNITE IN QUESTA SEDE, TUTTI I FILE DI DOCUMENTI E IL SOFTWARE DI TALI FORNITORI VENGONO FORNITI "COME SONO" CON TUTTI GLI ERRORI. CISCO E I SUDDETTI FORNITORI NON CONCEDONO NESSUN'ALTRA GARANZIA, ESPLICITA O IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, QUELLE DI COMMERCIABILITÀ, IDONEITÀ A UNO SCOPO SPECIFICO E DI NON VIOLAZIONE DEI DIRITTI ALTRUI, O DERIVANTI DA UNA PRATICA DI NEGOZIAZIONE, UTILIZZO O VENDITA.

IN NESSUN CASO CISCO O I SUOI FORNITORI SARANNO RESPONSABILI DI EVENTUALI DANNI INDIRETTI, SPECIALI, CONSEQUENZIALI O INCIDENTALI, INCLUSI, SENZA LIMITAZIONI, LA PERDITA DI PROFITTI O LA PERDITA O IL DANNEGGIAMENTO DI DATI DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE QUESTO MANUALE, ANCHE QUALORA CISCO O I SUOI FORNITORI SIANO STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI.

Tutti gli indirizzi Internet Protocol (IP) e i numeri di telefono utilizzati in questo documento non sono indirizzi e numeri di telefono reali. Tutti gli esempi, i risultati di visualizzazione dei comandi, i diagrammi di topologia di rete e le immagini inclusi nel documento vengono mostrati solo a titolo illustrativo. L'utilizzo di indirizzi IP o numeri di telefono reali nei contenuti delle illustrazioni non è voluto ed è del tutto casuale.

Tutte le copie stampate e tutti i duplicati elettronici del presente documento sono da considerarsi non controllati. Per la versione più recente, vedere l'ultima versione online.

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono sono disponibili nel sito Web Cisco all'indirizzo www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

SOMMARIO

Prefazione

Panoramica

La Guida all'amministrazione del *telefono IP Cisco serie 8800 per Cisco Unified Communications Manager* fornisce le informazioni necessarie per comprendere, installare, configurare, gestire e per la risoluzione dei problemi dei telefoni in una rete VoIP.

A causa della complessità della rete di telefonia IP, questa guida non fornisce informazioni complete e dettagliate per le procedure che occorre eseguire in Cisco Unified Communications Manager o in altri dispositivi di rete.

Destinatari

Si consiglia agli ingegneri di rete, agli amministratori del sistema e agli ingegneri delle telecomunicazioni di consultare questa guida per apprendere le procedure richieste per l'impostazione dei telefoni IP Cisco. Per le attività descritte nel presente documento è necessario completare delle procedure di configurazione delle impostazioni di rete non destinate agli utenti del telefono. Tali attività richiedono dimestichezza con Cisco Unified Communications Manager.

Convenzioni della guida

Questo documento utilizza le seguenti convenzioni:

Convenzione	Descrizione
Grassetto	I comandi e le parole chiave sono in **grassetto**.
carattere *corsivo*	Gli argomenti per i quali vengono forniti dei valori sono in *corsivo*.

Convenzione	Descrizione
[]	Gli elementi tra parentesi quadre sono facoltativi.
{x | y | z}	Le parole chiave alternative sono inserite tra parentesi graffe e separate da barre verticali.
[x | y | z]	Le parole chiave alternative opzionali sono inserite tra parentesi quadre e separate da barre vert
stringa	Un set di caratteri non tra virgolette. Non utilizzare le virgolette intorno alla stringa oppure stringa includerà le virgolette.
Carattere dello `schermo`	Le sessioni del terminale e le informazioni visualizzate dal sistema sono riportate nel caratte dello `schermo`.
Carattere di **`inserimento`**	Le informazioni da immettere sono riportate nel carattere di **`inserimento`**.
Carattere dello *schermo in corsivo*	Gli argomenti per i quali vengono forniti dei valori sono nel carattere dello *schermo in cors*
^	Il simbolo ^ rappresenta il tasto Controllo, ad esempio la combinazione di tasti ^D nello sch significa tenere premuto il tasto Controllo mentre si preme il tasto D.
<>	I caratteri non stampabili, ad esempio le password, sono inseriti tra parentesi angolari.

Nota Significa *prendere nota*. Le note contengono suggerimenti utili o riferimenti a materiali non trattati nella pubblicazione.

Attenzione Significa *fare attenzione*. In questa situazione, è possibile che si stia per compiere un'operazione che potrebbe determinare un danneggiamento di un dispositivo o una perdita di dati.

Per gli avvisi viene utilizzata la convenzione seguente:

Attennzione ISTRUZIONI IMPORTANTI SULLA SICUREZZA

Il simbolo di avviso indica pericolo. Si è in una situazione che potrebbe causare danni fisici. Prima di utilizzare una qualsiasi apparecchiatura, assicurarsi di essere a conoscenza dei rischi legati ai circuiti elettrici e di avere dimestichezza con le procedure standard di prevenzione degli infortuni. Utilizzare il numero specificato alla fine di ciascun avviso per individuare la relativa traduzione negli avvisi di sicurezza tradotti forniti con questo dispositivo. Dichiarazione 1071.

CONSERVARE QUESTE ISTRUZIONI

Documentazione correlata

Utilizzare le sezioni indicate di seguito per le relative informazioni.

Documentazione di Telefono IP Cisco serie 8800

Trovare la documentazione specifica per la lingua, il modello di telefono e il sistema di controllo delle chiamate nella pagina di supporto del prodotto per il telefono IP Cisco serie 7800.

La Guida alla distribuzione è disponibile al seguente URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Documentazione di Cisco Unified Communications Manager

Consultare la *Cisco Unified Communications ManagerGuida alla documentazione* e altre pubblicazioni specifiche della versione Cisco Unified Communications Manager in uso. Consultare l'URL della documentazione indicato di seguito:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Documentazione di Cisco Business Edition 6000

Consultare la Guida di *Cisco Business Edition 6000* e altre pubblicazioni specifiche della versione di Cisco Business Edition 6000 in uso. Consultare l'URL indicato di seguito:

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

Documentazione, supporto e linee guida di sicurezza

Per informazioni sulla richiesta di documentazione e di assistenza, su come inviare feedback sulla documentazione, sulla revisione delle linee guida di sicurezza, nonché sugli alias consigliati e sui documenti Cisco di carattere generale, si rimanda alla pubblicazione mensile *What's New in Cisco Product Documentation*, che offre inoltre un elenco di tutta la documentazione tecnica nuova e aggiornata di Cisco, all'indirizzo:

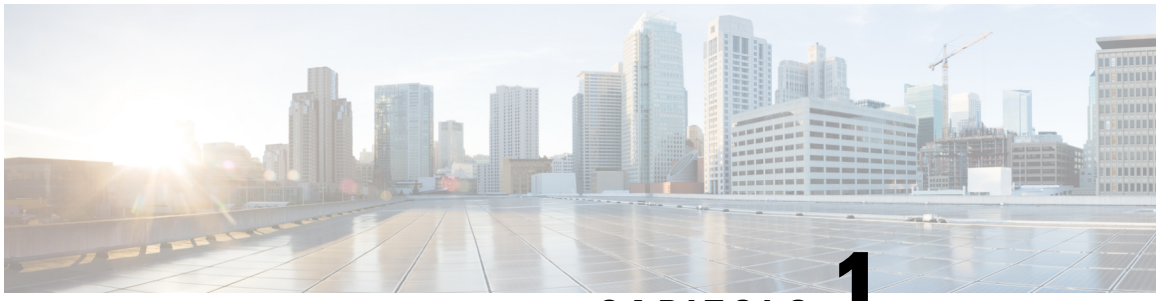
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Effettuare l'iscrizione alla pubblicazione *What's New in Cisco Product Documentation* come feed RSS (Really Simple Syndication) e utilizzare i relativi contenuti direttamente dal desktop tramite un'applicazione di lettura. I feed RSS sono un servizio gratuito e Cisco supporta attualmente RSS versione 2.0.

Informazioni generali sulla protezione del prodotto Cisco

Il presente prodotto contiene funzionalità di crittografia ed è soggetto alle leggi vigenti negli Stati Uniti e nel paese locale che regolamentano l'importazione, l'esportazione, il trasferimento e l'uso. La distribuzione di prodotti con crittografia Cisco non conferisce a terze parti l'autorizzazione a importare, esportare, distribuire o utilizzare la crittografia. Gli importatori, gli esportatori, i distributori e gli utenti hanno la responsabilità di rispettare le leggi vigenti negli Stati Uniti e nel paese locale. Utilizzando questo prodotto si accetta di rispettare le leggi e le normative applicabili. In caso di mancata conformità alle leggi degli Stati Uniti e alle leggi locali, restituire immediatamente il prodotto.

Ulteriori informazioni relative alle normative sull'esportazione degli Stati Uniti sono disponibili all'indirizzo https://www.bis.doc.gov/policiesandregulations/ear/index.htm.



CAPITOLO 1

Novità e modifiche

Novità e modifiche per la versione del firmware 14.2(1)

Le informazioni riportate di seguito sono nuove o modificate per la versione del firmware 14.2(1).

Funzione	Novità o modifiche
Supporto per SIP OAuth su SRST	Miglioramento della protezione della rete telefonica, a pagina 87
Semplificazione dell'accesso a Extension Mobility con l'adattatore USB per la cuffia Cisco 730	Funzioni del telefono, a pagina 124
Sincronizzazione della disattivazione dell'audio Bluetooth per la cuffia Cisco serie 700	Funzioni del telefono, a pagina 124
Nuove impostazioni per la cuffia Cisco serie 500: Evento nell'alloggiamento e modalità Sempre attivo	Funzioni del telefono, a pagina 124

Novità e modifiche per la versione del firmware 14.1(1)

Le informazioni riportate di seguito sono nuove o modificate per la versione del firmware 14.1(1).

Funzione	Novità o modifiche
Supporto di SIP OAuth per Proxy TFTP	Miglioramento della protezione della rete telefonica, a pagina 87
Avviso di chiamata migliorato per il gruppo di ricerca	Funzioni del telefono, a pagina 124
Visualizzazione del numero di chiamata configurabile per la modalità linea avanzata	Configurazione specifica del prodotto
PLAR ritardato configurabile	Funzioni del telefono, a pagina 124
Supporto di MRA per l'accesso a Extension Mobility con cuffie Cisco	Funzioni del telefono, a pagina 124
Migrazione del telefono senza caricamento di transizione	Migrazione diretta del telefono a un telefono multipiattaforma, a pagina 197

Novità e modifiche per la versione del firmware 14.0(1)

Tabella 1: Novità e modifiche

Funzione	Novità o modifiche
Miglioramento del monitoraggio del parcheggio di chiamata	Configurazione specifica del prodotto, a pagina 146
Miglioramenti a SIP OAuth	Miglioramento della protezione della rete telefonica, a pagina 87
Miglioramenti dell'interfaccia utente	SRST (Survivable Remote Site Telephony), a pagina 77 Funzioni del telefono, a pagina 124
Miglioramenti a OAuth per MRA	Mobile and Remote Access Through Expressway, a pagina 181

A partire dalla versione del firmware 14.0, i telefoni supportano DTLS 1.2. DTLS 1.2 richiede Cisco Adaptive Security Appliance (ASA) versione 9.10 o successive. È possibile configurare la versione minima di DTLS per una connessione VPN in ASA. Per ulteriori informazioni, vedere *ASDM Book 3: Guida alla configurazione di Cisco ASA serie VPN ASDM* all'indirizzo https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Novità e modifiche per la versione del firmware 12.8(1)

Le informazioni riportate di seguito sono nuove o modificate per la versione 12.8(1) del firmware.

Funzione	Contenuti nuovi o modificati
Migrazione dei dati del telefono	Modifica del modello del telefono di un utente, a pagina 67
Miglioramento aggiornamento cuffia	Informazioni dispositivo, a pagina 238
Semplificazione dell'accesso a Extension Mobility con cuffie Cisco	Funzioni del telefono, a pagina 124
Modifiche del controllo delle funzioni	Configurazione specifica del prodotto, a pagina 146, nuovi campi **Avviso abbassa la voce** e **Contrassegna la chiamata come spam**
Modifiche generali	Chiarire Wi-Fi e la porta PC: • Impostazione del telefono dai menu di configurazione, a pagina 49 • Abilitazione della LAN wireless sul telefono, a pagina 51
Aggiunta di ulteriori informazioni sul campo Accesso Web	Configurazione specifica del prodotto, a pagina 146
Rimozione della funzione non supportata	Funzioni del telefono, a pagina 124

Novità e modifiche per la versione del firmware 12.7(1)

Tabella 2: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.7(1)

Revisione	Sezione aggiornata
Aggiornata per supporto dello sfondo sui moduli di espansione tasti.	Immagini di sfondo personalizzate, a pagina 117
Aggiornata per il supporto della Cuffia Cisco 730	Informazioni dispositivo, a pagina 238
Aggiornata per la versione del firmware 2.0 della Cuffia Cisco serie 500	Informazioni dispositivo, a pagina 238 Gestione delle cuffie sulle versioni precedenti di Cisco Unified Communications Manager, a pagina 210
Aggiornata per le chiamate del gruppo di ricerca in arrivo.	Funzioni del telefono, a pagina 124

Revisione	Sezione aggiornata
Le informazioni sulla configurazione dello sgancio elettronico sono state rimosse.	Configurazione specifica del prodotto, a pagina 146

Novità e modifiche per la versione del firmware 12.6(1)

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 3: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.6(1)

Revisione	Sezione aggiornata
Aggiornata per il ripristino della linea principale in modalità linea sessione	Configurazione specifica del prodotto, a pagina 146 Ambiente in modalità linea sessione, a pagina 168

Novità per la versione del firmware 12.5(1)SR3

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 4: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.5(1)SR3

Revisione	Sezione aggiornata
Supporto per l'onboarding tramite codice di attivazione e l'accesso mobile e remoto	Onboarding tramite codice di attivazione e accesso mobile e remoto, a pagina 45
Supporto per l'utilizzo dello strumento di segnalazione dei problemi (PRT) in Cisco Unified Communications Manager.	Creazione di un rapporto sul problema del telefono in Cisco Unified Communications Manager, a pagina 269
Nuovo paragrafo	Condivisione della connessione di rete con il telefono e il computer, a pagina 49
Nuovo paragrafo	Protezione della videocamera del telefono, a pagina 39

Novità per la versione del firmware 12.5(1)SR1

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 5: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.5(1)SR1

Revisione	Sezione aggiornata
Supporto per crittografia a curva ellittica	Funzioni di protezione supportate, a pagina 88
Supporto per miglioramenti alla cronologia delle chiamate per modalità di linea avanzata con linee di rollover	Funzioni disponibili in modalità linea avanzata, a pagina 205
Supporto per messaggi privati su Cisco Unified Communications Manager Express	Interazione con Cisco Unified Communications Manager Express, a pagina 23
Supporto per la lingua cinese	Limitazione di lingua, a pagina 284
Supporto per l'onboarding tramite codice di attivazione	Onboarding tramite codice di attivazione per telefoni in sede, a pagina 44
Supporto per percorsi dei supporti e Interactive Connectivity Establishment	Percorsi di supporti e Interactive Connectivity Establishment, a pagina 183
Supporto per la disabilitazione delle crittografie TLS	Configurazione specifica del prodotto, a pagina 146
Supporto per la disabilitazione del ricevitore in modo da mantenere il percorso audio sulla cuffia	Configurazione specifica del prodotto, a pagina 146
Supporto per la configurazione remota dei parametri della cuffia	Gestione delle cuffie sulle versioni precedenti di Cisco Unified Communications Manager, a pagina 210

Novità per la versione del firmware 12.1(1)SR1

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 6: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.1(1)SR1

Revisione	Sezione aggiornata
Composizione Enbloc per il miglioramento del timer di interdigitazione T.302.	Configurazione specifica del prodotto, a pagina 146

Novità per la versione del firmware 12.1(1)

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 7: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware12.1(1)

Revisione	Sezione aggiornata
L'accesso mobile e remoto tramite Expressway ora supporta la modalità linea avanzata.	Funzioni del telefono disponibili per Mobile and Remote Access Through Expressway, a pagina 183
	Mobile and Remote Access Through Expressway, a pagina 181
	Funzioni disponibili in modalità linea avanzata, a pagina 205
Ora è supportata l'abilitazione o la disabilitazione di TLS 1.2 per l'accesso al server Web.	Configurazione specifica del prodotto, a pagina 146
Il codec audio G722.2 AMR-WB è attualmente supportato.	Panoramica sul telefono, a pagina 29
	Campi di Statistiche chiamate, a pagina 233

Novità per la versione del firmware 12.0(1)

Tutte le nuove funzioni sono state aggiunte a Funzioni del telefono, a pagina 124.

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 8: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 12.0(1)

Revisione	Sezione aggiornata
Aggiornata per il supporto di Parcheggio chiamata, Stato linea Parcheggio chiamata, Risposta per assente di gruppo e Gruppi di ricerca in modalità linea avanzata	Funzioni disponibili in modalità linea avanzata, a pagina 205

Novità per la versione del firmware 11.7(1)

Non è stato necessario aggiornare la Guida all'amministrazione per la versione del firmware 11.7(1).

Novità per la versione del firmware 11.5(1)SR1

Tutte le nuove funzioni sono state aggiunte a Funzioni del telefono, a pagina 124.

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

Tabella 9: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 11.5(1)SR1

Revisione	Sezione aggiornata
Aggiornata per il supporto del telefono IP Cisco 8865NR	• Requisiti di alimentazione dei telefoni, a pagina 16 • Protocolli di rete, a pagina 18 • Panoramica sul telefono, a pagina 29 • Pulsanti e hardware, a pagina 36
Aggiornata per il supporto di registrazione e monitoraggio in modalità linea avanzata	Funzioni disponibili in modalità linea avanzata, a pagina 205
Aggiornata per il supporto dell'elenco di ricerca WLAN	Abilitazione della LAN wireless sul telefono, a pagina 51
	Impostazione della LAN Wireless dal telefono, a pagina 53
	Configurazione delle impostazioni di rete, a pagina 59
Aggiornata per il supporto della funzione Non disturbare con MLPP	Impostazione dell'opzione Non disturbare, a pagina 175
Aggiornata per il supporto della suoneria configurabile	Configurazione specifica del prodotto, a pagina 146
Protezione migliorata	Miglioramento della protezione della rete telefonica, a pagina 87
Modifiche generali	Aggiornamenti Pagina Web del telefono IP Cisco, a pagina 237 Nuova presentazione della configurazione delle funzioni del telefono in Cisco Unified Communications Manager Configurazione delle funzioni del telefono, a pagina 144

Novità per la versione del firmware 11.5(1)

Tabella 10: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 11.5(1).

Revisione	Sezione aggiornata
La modalità linea avanzata è supportata.	Impostazione di tasti di linea aggiuntivi, a pagina 204 Funzioni disponibili in modalità linea avanzata, a pagina 205
La funzione Non disturbare (NoDist) è stata aggiornata per una nuova visualizzazione.	Impostazione dell'opzione Non disturbare, a pagina 175

Revisione	Sezione aggiornata
Il codec OPUS è supportato.	Panoramica sul telefono, a pagina 29
La modalità FIPS è stata aggiunta.	Abilitazione della modalità FIPS, a pagina 94
L'impostazione WLAN è stato aggiornata.	Impostazione della LAN Wireless dal telefono, a pagina 53
Il profilo WLAN per i telefoni IP Cisco 8861 e 8865 è supportato.	Impostazione di un profilo Wi-Fi utilizzando Cisco Unified Communications Manager, a pagina 56
	Impostazione di un gruppo Wi-Fi utilizzando Cisco Unified Communications Manager, a pagina 58
L'impostazione dei tentativi di autenticazione WLAN è supportata.	Impostazione del numero di tentativi di autenticazione WLAN, a pagina 55
L'abilitazione della modalità prompt WLAN è supportata.	Abilitazione della modalità prompt WLAN, a pagina 56
È supportata la personalizzazione del segnale di linea.	Personalizzazione del segnale di linea, a pagina 121
La visualizzazione della schermata Informazioni sulla rete è supportata.	Visualizzazione della schermata Informazioni sulla rete, a pagina 227

Novità per la versione del firmware 11.0

Tutte le nuove funzioni sono state aggiunte a Funzioni del telefono, a pagina 124.

Tutti i riferimenti nella documentazione di Cisco Unified Communications Manager sono stati aggiornati per supportare tutte le versioni di Cisco Unified Communications Manager.

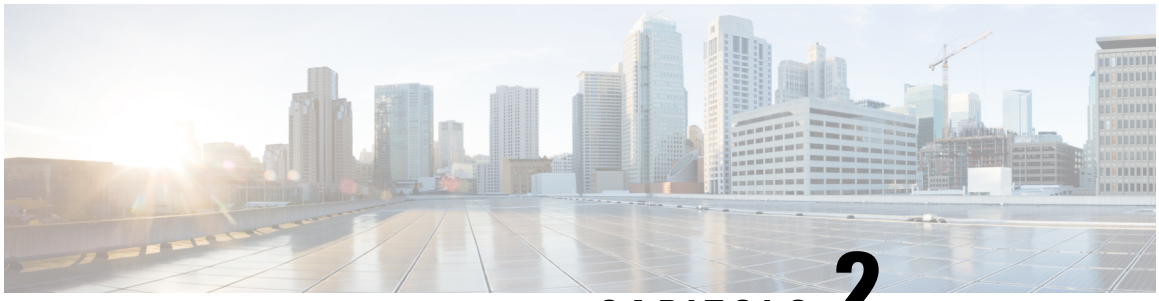
Tabella 11: Revisioni della Guida all'amministrazione del telefono IP Cisco 8800 per la versione del firmware 11.0

Revisione	Sezione aggiornata
Aggiornata per chiarimenti e per risolvere le carenze	• Configurazione VPN, a pagina 203 • Configurazione delle impostazioni di rete, a pagina 59 • Impostazione di Energy Efficient Ethernet per la porta PC e dello switch, a pagina 179 • Impostazione della risoluzione di trasmissione del video, a pagina 209 • Enhanced Survivable Remote Site Telephony, a pagina 80
Aggiornata per il miglioramento del supporto dell'opzione di debug del telefono di sezione	• Controllo delle informazioni di debug da Cisco Unified Communications Manager, a pagina 274.

Revisione	Sezione aggiornata
Aggiornata per il miglioramento del supporto dei certificati digitali EAP-TLS + SCEP, PEAP-GTC e X.509	• Protezione WLAN, a pagina 97. • Impostazione della modalità di autenticazione, a pagina 101 • Credenziali di protezione wireless, a pagina 101
Aggiornata per il miglioramento del supporto dello Strumento di segnalazione problemi (PRT)	• Problem Reporting Tool (PRT), a pagina 186. • Configurazione di un URL di caricamento assistenza clienti, a pagina 186.
Aggiunta per il supporto della Regola di composizione applicazione	• Regole di composizione applicazione, a pagina 80
Aggiunto per etichetta di testo linea	• Impostazione di un'etichetta per una linea, a pagina 187.

PARTE I

Informazioni sul telefono IP Cisco



CAPITOLO 2

Dettagli tecnici

Specifiche fisiche e dell'ambiente operativo

Nella tabella seguente vengono elencate le specifiche fisiche e dell'ambiente operativo del telefono IP Cisco serie 8800.

Tabella 12: Specifiche fisiche e operative

Specifica	Valore o intervallo
Temperatura di esercizio	Da 0 °C a 40 °C (da 32 °F a 104 °F)
Umidità relativa di funzionamento	In funzionamento: dal 10% al 90% (senza condensa) Non in funzionamento: dal 10% al 95% (senza condensa)
Temperatura di conservazione	Da 10 °C a 60 °C (da 14 °F a 140 °F)
Altezza	229,1 mm (9,02 in.)
Larghezza	257,34 mm (10,13 in.)

Specifica	Valore o intervallo
Profondità	40 mm (1,57 in.)
Peso	1,19 kg (2,62 lb)
Alimentazione	100-240 V CA, 50-60 Hz, 0,5 A con adattatore CA 48 V CC, 0,2 A con alimentazione in linea tramite cavo di rete
Cavi	Cavi di categoria 3/5/5e/6 per 10-Mbps con 4 coppie Cavi di categoria 5/5e/6 per 100-Mbps con 4 coppie Cavi di categoria 5e/6 per 1000-Mbps con 4 coppie **Nota** I cavi hanno 4 coppie di fili per un totale di 8 conduttori.
Requisiti di distanza	Come supportato dalla Specifica Ethernet, si presume che la lunghezza massim tra ciascun telefono IP Cisco e lo switch sia di 100 metri.

Specifiche del cavo

Le informazioni seguenti elencano le specifiche dei cavi:

- Jack RJ-9 (4 conduttori) per connessione del ricevitore e della cuffia
- Jack RJ-45 per connessione LAN 10/100/1000BaseT (porta di rete 10/100/1000 sul telefono)
- Jack RJ-45 per una seconda connessione conforme 10/100/1000BaseT (porta di rete 10/100/1000 sul telefono)
- Jack di 3,5 mm per la connessione degli altoparlanti (solo per il telefono IP Cisco 8861)
- Connettore di alimentazione 48 V
- Porte/connettore USB: una porta USB sul telefono IP Cisco 8851 e due porte USB sul telefono IP Cisco 8861
- 3 connettori di moduli di espansione tasti, considerati come connettore USB per i telefoni IP Cisco 8851 e 8861.

Disposizione dei pin delle porte di rete e computer

Sebbene le porte di rete e computer (di accesso) vengano utilizzate per la connettività di rete, i loro scopi sono molteplici e la disposizione dei pin è diversa.

- La porta di rete corrisponde alla porta SW 10/100/1000 del telefono IP Cisco.
- La porta computer (di accesso) corrisponde alla porta PC 10/100/1000 del telefono IP Cisco.

Connettore porta di rete

Nella tabella seguente vengono descritte le disposizioni dei pin del connettore porta di rete.

Tabella 13: Disposizioni dei pin del connettore porta di rete

Numero pin	Funzione
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Nota	Per BI si intende "bidirezionale", mentre per DA, DB, DC e DD si intende rispettivamente "Dati A", "Dati B", "Dati C" e "Dati D".

Connettore porta del computer

Nella tabella seguente vengono descritte le disposizioni dei pin del connettore porta del computer.

Tabella 14: Disposizioni dei pin del connettore porta (di accesso) del computer

Numero pin	Funzione
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Nota	Per BI si intende "bidirezionale", mentre per DA, DB, DC e DD si intende rispettivamente "Dati A", "Dati B", "Dati C" e "Dati D".

Requisiti di alimentazione dei telefoni

È possibile alimentare il telefono IP Cisco con alimentazione esterna o tramite PoE (Power over Ethernet). Un alimentatore separato fornisce l'alimentazione esterna. Lo switch può fornire PoE tramite il cavo Ethernet del telefono.

Per supportare la funzionalità aggiuntive, i telefoni IP Cisco 8861 e 8865 sono dispositivi PoE di classe 4 e richiedono uno switch o una scheda di linea con funzionalità di classe 4.

Per ulteriori informazioni sui requisiti di alimentazione del telefono, consultare la scheda tecnica del telefono.

Quando si installa un telefono alimentato da un alimentatore esterno, collegare l'alimentatore prima di collegare il cavo Ethernet al telefono. Quando si rimuove un telefono alimentato da un alimentatore esterno, scollegare il cavo Ethernet dal telefono prima di scollegare l'alimentatore.

Tabella 15: Linee guida per l'alimentazione del telefono IP Cisco

Tipo di alimentazione	Linee guida
Alimentazione esterna: fornita tramite alimentazione esterna CP-PWR-CUBE-4=	Il telefono IP Cisco utilizza l'alimentatore CP-PWR-CUBE-4.
Alimentazione PoE: fornita da uno switch attraverso il cavo Ethernet collegato al telefono.	I telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR supportano PoE 802.3at per degli accessori. Per ulteriori informazioni, consultare la scheda tecnica del telefono. Per assicurare un funzionamento senza interruzioni del telefono, verificare che lo switch di un'alimentazione di backup. Assicurarsi che la versione CatOS o IOS eseguita sullo switch supporti l'implementa prevista del telefono. Per informazioni sulla versione del sistema operativo, consulta documentazione dello switch.
Universal Power Over Ethernet (UPoE)	I telefoni IP Cisco 8865 e 8865NR supportano UPoE.

I documenti riportati nella tabella seguente forniscono ulteriori informazioni sugli argomenti seguenti:

- Switch Cisco supportati dai telefoni IP Cisco
- Versione di Cisco IOS che supportano la negoziazione dell'alimentazione bidirezionale
- Altri requisiti e limitazioni di alimentazione

Tabella 16: Informazioni aggiuntive

Argomenti del documento	URL
Soluzioni PoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe
Switch Cisco Catalyst	http://www.cisco.com/c/en/us/products/switches/index.html

Argomenti del documento	URL
ISR (Integrated Services Router)	http://www.cisco.com/c/en/us/products/routers/index.html
Software Cisco IOS	http://www.cisco.com/c/en/us/products/ios-nx-os-software/inc

Interruzione dell'alimentazione

Per accedere al servizio di emergenza tramite il telefono è necessaria l'alimentazione del telefono. In caso di interruzione dell'alimentazione, non è possibile usufruire dell'assistenza o del servizio di chiamata di emergenza finché l'alimentazione non viene ripristinata. In caso di guasto o di interruzione dell'alimentazione, potrebbe essere necessario reimpostare o riconfigurare l'apparecchiatura per poter usufruire dell'assistenza o del servizio di chiamata di emergenza.

Consumi energetici ridotti

È possibile ridurre il consumo energetico del telefono IP Cisco tramite la modalità Risparmio energia o EnergyWise (Power Save Plus).

Risparmio energia

Nella modalità Risparmio energia, la retroilluminazione dello schermo non è attivata quando il telefono non è in uso. Il telefono rimane nella modalità Risparmio energia per la durata pianificata o fino a quando l'utente solleva il ricevitore o preme un pulsante qualsiasi.

Power Save Plus (EnergyWise)

Il telefono IP Cisco supporta la modalità EnergyWise (Power Save Plus). Se sulla rete è presente un controller EnergyWise (EW), ad esempio uno switch Cisco con la funzione EnergyWise abilitata, è possibile configurare i telefoni in base a una pianificazione di sospensione (spegnimento) e riattivazione (accensione) per ridurre ulteriormente il consumo energetico.

Impostare ciascun telefono sull'abilitazione o la disabilitazione delle impostazioni di EnergyWise. Se EnergyWise è abilitato, configurare un orario di sospensione e riattivazione, nonché altri parametri che verranno inviati al telefono come parte del file XML di configurazione del telefono.

Negoziazione alimentazione su LLDP

Il telefono e lo switch negoziano l'alimentazione consumata dal telefono. Il telefono IP Cisco funziona su diverse impostazioni di alimentazione che diminuiscono il consumo energetico quando è disponibile meno energia.

In seguito al riavvio del telefono, lo switch si blocca su un protocollo (CDP o LLDP) per la negoziazione dell'alimentazione. Lo switch si blocca sul primo protocollo (contenente un valore TLV [Threshold Limit Value]) trasmesso dal telefono. Se l'amministratore di sistema disabilita questo protocollo sul telefono, quest'ultimo non sarà in grado di accendere nessun accessorio perché lo switch non risponde alle richieste di alimentazione nell'altro protocollo.

Cisco consiglia di mantenere sempre abilitata (impostazione predefinita) la funzione Negoziazione alimentazione durante la connessione a uno switch in grado di supportarla.

Se questa funzione è disabilitata, lo switch potrebbe interrompere l'erogazione dell'alimentazione al telefono. Se lo switch non supporta la negoziazione dell'alimentazione, disabilitare la relativa funzione prima di accendere

gli accessori su PoE. Se la funzione Negoziazione alimentazione è disabilitata, il telefono può accendere gli accessori fino al massimo consentito dallo standard IEEE 802.3af-2003.

Nota

- Se il protocollo CDP e la funzione Negoziazione alimentazione sono disabilitati, il telefono può alimentare gli accessori fino a 15,4 W.

Protocolli di rete

I telefoni IP Cisco serie 8800 supportano più standard di settore e protocolli di rete Cisco richiesti per la comunicazione vocale. Nella tabella seguente viene fornita una panoramica dei protocolli di rete supportati dai telefoni.

Tabella 17: Protocolli di rete supportati dal telefono IP Cisco serie 8800

Protocollo di rete	Scopo	Note per l'utilizzo
Bluetooth	Il Bluetooth è un protocollo WPAN (Wireless Personal Area Network) che specifica le modalità di comunicazione tra dispositivi su brevi distanze.	I telefoni IP Cisco 8845, 8865 e 8851 supportano il Bluetooth 4.1. Il telefono IP Cisco 8861 supporta il Bluetooth 4.0. I telefoni IP Cisco 8811, 8841, 8851NR e 8865NR non supportano il Bluetooth.
Bootstrap Protocol (BootP)	Il protocollo BootP consente a un dispositivo di rete, come il telefono IP Cisco, di rilevare determinate informazioni di avvio, ad esempio l'indirizzo IP.	—
Cisco Audio Session Tunnel (CAST)	Il protocollo CAST consente ai telefoni e alle applicazioni associate di comunicare con i telefoni IP remoti senza richiedere modifiche ai componenti di segnalazione.	Il telefono IP Cisco utilizza CAST come interfaccia tra CUVA e Cisco Unified Communications Manager dove il telefono IP Cisco funge da proxy SIP.
CDP (Cisco Discovery Protocol)	CDP è un protocollo di rilevamento dispositivo eseguito su tutte le apparecchiature prodotte da Cisco. Tramite CDP, un dispositivo può comunicare la propria presenza ad altri dispositivi e ricevere informazioni sugli altri dispositivi in rete.	I telefoni IP Cisco utilizzano il protocollo CDP per scambiare informazioni quali l'ID della VLAN ausiliaria, i dettagli di gestione energetica per porta e le informazioni di configurazione QoS (Quality of Service) con lo switch Cisco Catalyst.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP è un protocollo proprietario di Cisco utilizzato per la creazione di una gerarchia peer-to-peer dei dispositivi. Questa gerarchia viene utilizzata per distribuire i file del firmware dai dispositivi peer ai dispositivi adiacenti.	Il protocollo CPPDP viene utilizzato dalla funzione Condivisione del firmware.

Protocollo di rete	Scopo	Note per l'utilizzo
Dynamic Host Configuration Protocol (DHCP)	DHCP alloca e assegna dinamicamente un indirizzo IP ai dispositivi di rete. Il protocollo DHCP consente di collegare un telefono IP alla rete e di rendere operativo il telefono senza dover assegnare manualmente un indirizzo IP o configurare parametri di rete aggiuntivi.	DHCP è abilitato per impostazione predefinita. Se è disabilitato, occorre configurare manualmente indirizzo IP, subnet mask, gateway e un server TFTP localmente su ogni telefono. Si consiglia di utilizzare l'opzione personalizzata DHCP 150. Con questo metodo, si configura l'indirizzo IP del server TFTP come valore dell'opzione. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso. **Nota** Se non è possibile utilizzare l'opzione 150, provare a utilizzare l'opzione DHCP 66.
Hypertext Transfer Protocol (HTTP)	HTTP è il metodo di trasferimento standard di informazioni e di spostamento di documenti su Internet e nel Web.	I telefoni IP Cisco utilizzano HTTP per i servizi XML e per la risoluzione dei problemi.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS (Hypertext Transfer Protocol Secure) è una combinazione del protocollo Hypertext Transfer Protocol con il protocollo SSL/TLS per fornire crittografia e identificazione sicura dei server.	Le applicazioni Web con supporto HTTP e HTTPS dispongono di due URL configurati. I telefoni IP Cisco che supportano HTTPS utilizzano l'URL HTTPS.
IEEE 802.1x	Lo standard IEEE 802.1X definisce un controllo degli accessi su base client-server e un protocollo di autenticazione che limita ai client non autorizzati la connessione a una LAN attraverso porte accessibili pubblicamente. Fino all'autenticazione del client, il controllo degli accessi 802.1X consente solo il traffico EAPOL (Extensible Authentication Protocol over LAN) attraverso la porta a cui è collegato il client. In seguito alla riuscita dell'autenticazione, il traffico normale può passare attraverso questa porta.	Il telefono IP Cisco implementa lo standard IEEE 802.1X tramite il supporto per i seguenti metodi di autenticazione: EAP-FAST ed EAP-TLS. Se l'autenticazione 802.1X è abilitata sul telefono, occorre disabilitare la porta PC e la VLAN vocale.
IEEE 802.11n/802.11ac	Lo standard IEEE 802.11 specifica le modalità di comunicazione tra dispositivi su una rete locale wireless (WLAN). 802.11n funziona sulle bande 2,4 GHz e 5 GHz, mentre 802.11ac sulla banda 5 GHz.	L'interfaccia 802.11 è un'opzione di implementazione per i casi in cui il cablaggio Ethernet non fosse disponibile o desiderato. Solo il telefono IP Cisco 8861 e 8865 supportano la WLAN.

Protocollo di rete	Scopo	Note per l'utilizzo
Protocollo Internet (IP)	IP è un protocollo di messaggistica che indirizza e invia pacchetti in rete.	Per comunicare tramite il protocollo IP, i dispositivi di rete devono disporre di indirizzo IP, subnet e gateway assegnati. Se si utilizza il telefono IP Cisco con Dynamic Host Configuration Protocol (DHCP), le identificazioni di indirizzi IP, subnet e gateway vengono assegnate automaticamente. Se non si utilizza DHCP, occorre assegnare manualmente queste proprietà localmente a ciascun telefono. I telefoni IP Cisco supportano gli indirizzi IPv6. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Protocollo LLDP (Link Layer Discovery Protocol)	LLDP è un protocollo di rilevamento di rete standardizzato (simile a CDP) supportato su alcuni dispositivi Cisco e di terze parti.	Il telefono IP Cisco supporta LLDP sulla porta PC.
Protocollo LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	Il protocollo LLDP-MED è un'estensione dello standard LLDP sviluppato per i prodotti vocali.	Il telefono IP Cisco supporta LLDP-MED sulla porta SW per comunicare informazioni quali: • Configurazione VLAN vocale • Rilevamento dei dispositivi • Gestione energetica • Gestione delle scorte
RTP (Real-Time Transport Protocol)	RTP è un protocollo standard per il trasporto dei dati in tempo reale, come voce e video interattivi, su reti dati.	I telefoni IP Cisco utilizzano il protocollo RTP per inviare e ricevere traffico vocale in tempo reale da altri telefoni e gateway.
Protocollo RTCP (Real-Time Control Protocol)	RTCP funziona insieme a RTP per fornire dati QoS (come jitter, latenza e ritardo round trip) su flussi RTP.	RTCP è abilitato per impostazione predefinita.
Protocollo Session Description Protocol (SDP)	SDP è la porzione del protocollo SIP che determina i parametri disponibili durante una connessione tra due endpoint. Le conferenze vengono stabilite utilizzando soltanto le capacità SDP supportate da tutti gli endpoint nella conferenza.	Le capacità SDP, come ad esempio i tipi di codec, il rilevamento DTMF e il rumore di comfort, vengono solitamente configurate su base globale da Cisco Unified Communications Manager o da Media Gateway durante il funzionamento. Alcuni endpoint SIP possono consentire la configurazione di tali parametri direttamente sull'endpoint.

Protocollo di rete	Scopo	Note per l'utilizzo
Protocollo SIP (Session Initiation Protocol)	SIP è lo standard Internet Engineering Task Force (IETF) per conferenze multimediali su IP. SIP è un protocollo di controllo a livello di applicazione basato su ASCII (definito in RFC 3261) utilizzabile per stabilire, mantenere e terminare le chiamate tra due o più endpoint.	Analogamente ad altri protocolli VoIP, SIP include tutte le funzioni di gestione della segnalazione e delle sessioni all'interno di una rete di telefonia a pacchetti. La segnalazione consente il trasporto delle informazioni sulla chiamata oltre i confini della rete. La gestione delle sessioni consente di controllare gli attributi di una chiamata end-to-end. I telefoni IP Cisco supportano il protocollo SIP se vengono attivati solo sull'indirizzo IPv6, solo sull'indirizzo IPv4 o sugli indirizzi IPv4 e IPv6.
Protocollo TCP (Transmission Control Protocol)	TCP è un protocollo di trasporto orientato alla connessione.	I telefoni IP Cisco utilizzano il protocollo TCP per il collegamento a Cisco Unified Communications Manager e per l'accesso ai servizi XML.
Protocollo TLS (Transport Layer Security)	TLS è un protocollo standard per la protezione e l'autenticazione delle comunicazioni.	Durante l'implementazione della protezione, i telefoni IP Cisco utilizzano il protocollo TLS per la registrazione protetta su Cisco Unified Communications Manager.
Protocollo TFTP (Trivial File Transfer Protocol)	TFTP consente di trasferire i file in rete. Sul telefono IP Cisco, TFTP consente di ottenere un file di configurazione specifico per il tipo di telefono.	Il protocollo TFTP richiede la presenza di un server TFTP nella rete che può essere identificato automaticamente dal server DHCP. Se si desidera che il telefono utilizzi un server TFTP diverso da quello specificato dal server DHCP, occorre assegnare manualmente l'indirizzo IP del server TFTP mediante il menu Impostazione rete del telefono. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Protocollo UDP (User Datagram Protocol)	UDP è un protocollo di messaggistica senza connessione per la consegna dei pacchetti dati.	UDP viene utilizzato soltanto per i flussi RTP. La segnalazione SIP sui telefoni non supporta il protocollo UDP.

Per ulteriori informazioni sul supporto del protocollo LLDP-MED, consultare il white paper LLDP-MED and Cisco Discovery Protocol:

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml.

Argomenti correlati

Autenticazione 802.1X, a pagina 113
Configurazione delle impostazioni di rete
Verifica dell'avvio del telefono, a pagina 66
Interazione VLAN, a pagina 22
Interazione con Cisco Unified Communications Manager, a pagina 22
Interazione con Cisco Unified Communications Manager Express, a pagina 23

Impostazione dell'intervallo di porta audio e video, a pagina 191
Documentazione di Cisco Unified Communications Manager, a pagina xv

Interazione VLAN

Il telefono IP Cisco dispone di uno switch Ethernet interno che consente l'inoltro dei pacchetti al telefono, alla porta (di accesso) del computer e alla porta di rete posizionate sul retro del telefono.

Se un computer è connesso alla porta (di accesso) del computer, condivide con il telefono lo stesso collegamento fisico allo switch e la stessa porta sullo switch. Questo collegamento fisico condiviso ha le seguenti implicazioni per la configurazione VLAN sulla rete:

- È possibile configurare le VLAN correnti su una base subnet IP. Tuttavia, potrebbero non essere disponibili degli indirizzi IP aggiuntivi per assegnare il telefono alla stessa subnet degli altri dispositivi connessi alla stessa porta.
- Il traffico di dati presente sui telefoni con supporto della rete VLAN potrebbe ridurre la qualità del traffico VoIP.
- La sicurezza della rete potrebbe indicare la necessità di isolare il traffico vocale VLAN dal traffico di dati VLAN.

È possibile risolvere questi problemi isolando il traffico vocale in una VLAN separata. La porta dello switch a cui si connette il telefono viene quindi configurata su VLAN separate per il trasferimento del:

- Traffico vocale verso e dal telefono IP (ad esempio, VLAN ausiliaria su Cisco Catalyst serie 6000).
- Traffico di dati verso e dal PC connesso allo switch tramite la porta (di accesso) del computer del telefono IP (VLAN nativa).

L'isolamento dei telefoni su una VLAN separata e ausiliaria consente di aumentare la qualità del traffico vocale e di aggiungere più numeri di telefono a una rete esistente che non dispone di indirizzi IP sufficienti per ciascun telefono.

Per ulteriori informazioni, consultare la documentazione inclusa con lo switch Cisco. È possibile accedere alle informazioni sullo switch anche tramite l'URL:

http://cisco.com/en/US/products/hw/switches/index.html.

Interazione con Cisco Unified Communications Manager

Cisco Unified Communications Manager è un sistema di elaborazione delle chiamate aperto e standard del settore. Il software Cisco Unified Communications Manager consente di impostare ed eliminare le chiamate tra telefoni, integrando la funzionalità PBX tradizionale con la rete IP aziendale. Cisco Unified Communications Manager gestisce i componenti del sistema di telefonia, come ad esempio telefoni, gateway di accesso e le risorse necessarie per funzioni quali le chiamate in conferenza e la pianificazione dell'indirizzamento. Cisco Unified Communications Manager fornisce inoltre:

- Firmware per i telefoni
- File Certificate Trust List (CTL) e Identity Trust List (ITL) mediante i servizi TFTP e HTTP
- Registrazione dei telefoni

- Conservazione delle chiamate, per fare in modo che una sessione multimediale prosegua anche in caso di perdita del segnale tra il server di Communications Manager primario e il telefono

Per informazioni sulla configurazione di Cisco Unified Communications Manager sui telefoni descritti in questo capitolo, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Nota Se il modello del telefono che si desidera configurare non viene visualizzato nell'elenco a discesa Tipo telefono di Cisco Unified Communications Manager Administration, installare il pacchetto del dispositivo più recente per la versione di Cisco Unified Communications Manager in uso da Cisco.com.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Interazione con Cisco Unified Communications Manager Express

Quando il telefono è in funzione su Cisco Unified Communications Manager Express (Unified CME), deve attivarsi la modalità CME.

Quando un utente richiama la funzione conferenza, il tag consente al telefono di utilizzare un ponte conferenza hardware locale o di rete.

I telefoni non supportano le azioni seguenti:

- Trasferimento: supportato solo nello scenario di trasferimento della chiamata collegata.
- Conferenza: supportata solo nello scenario di trasferimento chiamata collegata.
- Collega: supportata tramite il pulsante Conferenza o l'accesso Hookflash.
- Attesa: supportata tramite il pulsante Attesa.
- Includi e Unisci: non supportata.
- Trasferimento diretto: non supportato.
- Seleziona: non supportata.

Gli utenti non possono creare conferenze e trasferire le chiamate tra linee diverse.

Unified CME supporta le chiamate interne, note anche come messaggi privati. Tuttavia, le chiamate tramite cercapersone vengono rifiutate dal telefono se è in corso una chiamata.

La modalità linea sessione e la modalità linea avanzata sono supportate in modalità CME.

Interazione con il sistema di voice messaging

Cisco Unified Communications Manager consente l'integrazione con diversi sistemi di voice messaging, incluso il sistema di voice messaging Cisco Unity Connection. Dal momento che è possibile effettuare l'integrazione con diversi sistemi, è necessario fornire agli utenti le informazioni sull'utilizzo del proprio sistema specifico.

Per abilitare la possibilità per un utente per il trasferimento alla casella vocale, impostare uno schema di composizione *xxxxx e configurarlo come inoltro di tutte le chiamate alla casella vocale. Per ulteriori informazioni, consultare la documentazione di Cisco Unified Communications Manager.

Fornire a ciascun utente le informazioni seguenti:

- Modalità di accesso all'account del sistema di voice messaging.

  Assicurarsi di aver utilizzato Cisco Unified Communications Manager per la configurazione del pulsante Messaggi sul telefono IP Cisco.

- Password iniziale per l'accesso al sistema di voice messaging.

  Configurare una password predefinita del sistema di messaggistica vocale per tutti gli utenti.

- Modalità di comunicazione della presenza di messaggi vocali da parte del telefono.

  Utilizzare Cisco Unified Communications Manager per l'impostazione di un metodo MWI (Message Waiting Indicator, indicatore di messaggio in attesa).

Panoramica dell'avvio del telefono

Durante la connessione alla rete VoIP, i telefoni IP Cisco seguono un processo di avvio standard. A seconda della configurazione specifica di rete, possono verificarsi soltanto alcuni dei passaggi seguenti sul telefono IP di Cisco.

1. Ricevere alimentazione dallo switch. Se il telefono non utilizza una fonte di alimentazione esterna, lo switch fornisce alimentazione interna tramite il cavo Ethernet collegato al telefono.
2. (Solo per i telefoni IP Cisco 8861 e 8865 in una rete LAN Wireless) Ricercare un punto di accesso. Il telefono IP Cisco 8861 e 8865 effettua la scansione dell'area di copertura RF con la radio. Il telefono ricerca i profili di rete ed effettua la scansione dei punti di accesso che contengono un SSID e un tipo di autenticazione corrispondenti. Il telefono effettua l'associazione con il punto di accesso con l'RSSI più elevato che corrisponde al profilo di rete.
3. (Solo per i telefoni IP Cisco 8861 e 8865 in una rete LAN wireless) Effettuare l'autenticazione sul punto di accesso. Il telefono IP Cisco avvia il processo di autenticazione. Nella tabella seguente viene descritto il processo di autenticazione:

Tipo di autenticazione	Opzioni di gestione chiavi	Descrizione
Aperta	Nessuno	Qualsiasi dispositivo può effettuare l'autenticazione sul punto di accesso. Per ulteriore protezione, se si desidera è possibile utilizzare la crittografia WEP.
Chiave condivisa	Nessuno	Prima che l'accesso alla rete sia disponibile, il telefono effettua la crittografia del testo di verifica tramite la chiave WEP e il punto di accesso deve verificare tale chiave utilizzata per crittografare il testo di verifica.
PEAP o EAP-FAST	Nessuno	Il server RADIUS autentica il nome utente e la password prima che l'accesso alla rete sia disponibile.

4. Caricare l'immagine del telefono memorizzata. All'avvio, il telefono esegue un caricatore bootstrap che carica un'immagine del firmware del telefono memorizzata nella memoria flash. Tramite questa immagine, il telefono inizializza il software e l'hardware.
5. Configurare la VLAN. Se il telefono IP Cisco è connesso a uno switch Cisco Catalyst, lo switch invia delle informazioni al telefono sulla VLAN vocale definita sullo switch. Prima che possa procedere con la richiesta Dynamic Host Configuration Protocol (DHCP) per un indirizzo IP, il telefono deve conoscere l'appartenenza VLAN.
6. Ottenere un indirizzo IP. Se il telefono IP Cisco utilizza il protocollo DHCP per ottenere un indirizzo IP, contatta il server DHCP per ottenerne uno. Se non si utilizza il protocollo DHCP nella rete, occorre assegnare degli indirizzi IP statici localmente a ciascun telefono.
7. Richiedere il file CTL. Il server TFTP memorizza il file CTL. Il file contiene i certificati necessari per stabilire una connessione protetta tra il telefono e Cisco Unified Communications Manager.

   Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
8. Richiedere il file ITL. Il telefono richiede il file ITL dopo aver richiesto il file CTL. Il file ITL contiene i certificati delle entità attendibili per il telefono. I certificati vengono utilizzati per autenticare una connessione protetta con i server o per autenticare la firma digitale dei server. Cisco Unified Communications Manager 8.5 e versioni successive supportano il file ITL.
9. Accedere a un server TFTP. Oltre ad assegnare un indirizzo IP, il server DHCP reindirizza il telefono IP Cisco a un server TFTP. Se il telefono dispone di un indirizzo IP definito staticamente, è necessario configurare il server TFTP in locale sul telefono; il telefono quindi contatta direttamente il server TFTP.

Nota È inoltre possibile assegnare un server TFTP alternativo da utilizzare al posto di quello assegnato dal server DHCP.

10. Richiedere il file di configurazione. Il server TFTP dispone di file di configurazione che definiscono i parametri per la connessione a Cisco Unified Communications Manager e altre informazioni sul telefono.
11. Contattare Cisco Unified Communications Manager. Il file di configurazione definisce in che modo il telefono IP Cisco comunica con Cisco Unified Communications Manager e fornisce l'ID di caricamento al telefono. Dopo aver ottenuto il file dal server TFTP, il telefono tenta di stabilire una connessione con il server Cisco Unified Communications Manager con la priorità più elevata presente nell'elenco.

    Se il profilo di protezione del telefono è configurato per la segnalazione protetta (crittografato o autenticato) e il server Cisco Unified Communications Manager è impostato sulla modalità protetta, il telefono stabilisce una connessione TLS. In caso contrario, il telefono stabilisce una connessione TCP non protetta.

    Cisco Unified Communications Manager identifica il telefono se quest'ultimo è stato aggiunto manualmente al database. Se il telefono non è stato aggiunto manualmente al database e in Cisco Unified Communications Manager è abilitata la registrazione automatica, il telefono tenta di registrarsi automaticamente nel database di Cisco Unified Communications Manager.

Nota La funzione di registrazione automatica è disabilitata se si configura il client CTL. In questo caso, è necessario aggiungere manualmente il telefono al database di Cisco Unified Communications Manager.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Dispositivi esterni

Si consiglia l'uso di dispositivi esterni di buona qualità protetti dai segnali di frequenza radio (RF) e frequenza audio (AF) indesiderati. I dispositivi esterni comprendono cuffie, cavi e connettori.

Eventuali interferenze audio dipendono dalla qualità di questi dispositivi e dalla relativa vicinanza ad altri dispositivi quali telefoni cellulari o radio a due frequenze. In questi casi, si consiglia di tentare di effettuare una o più delle seguenti operazioni:

- Allontanare il dispositivo esterno dall'origine dei segnali RF o AF.
- Allontanare i cavi del dispositivo esterno dall'origine dei segnali RF o AF.
- Utilizzare cavi schermati per il dispositivo esterno oppure utilizzare cavi con uno schermo e un connettore migliori.
- Ridurre la lunghezza del cavo del dispositivo esterno.
- Applicare ferriti o altri dispositivi simili sui cavi per il dispositivo esterno.

Cisco non può offrire garanzie sulle prestazioni di dispositivi esterni, cavi e connettori.

Attenzione Nei paesi dell'Unione Europea, utilizzare solo cuffie, microfoni e altoparlanti esterni pienamente conformi alla direttiva CEM (89/336/CEE) in materia di compatibilità elettromagnetica.

Informazioni sulla porta USB

I telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR supportano un massimo di cinque dispositivi che si connettono a ciascuna porta USB. Ciascun dispositivo collegato al telefono è incluso nel numero massimo di dispositivi. Ad esempio, il telefono può supportare cinque dispositivi USB sulla porta laterale e altri cinque dispositivi USB standard sulla porta posteriore. Molti prodotti USB di terze parti contano come più dispositivi USB, ad esempio un dispositivo contenente una cuffia e un hub USB può contare come due dispositivi USB. Per ulteriori informazioni, consultare la documentazione del dispositivo USB.

Nota

- Gli hub non alimentati e quelli alimentati con più di quattro porte non sono supportati.
- Le cuffie USB collegate al telefono tramite un hub USB non sono supportate.

Ciascun modulo di espansione tasti collegato al telefono viene contato come dispositivo USB. Se al telefono sono collegati tre moduli di espansione tasti, questi ultimi verranno conteggiati come tre dispositivi USB.

File di configurazione del telefono

I file di configurazione del telefono vengono memorizzati sul server TFTP e definiscono i parametri per la connessione a Cisco Unified Communications Manager. In generale, ogni volta che viene apportata una modifica in Cisco Unified Communications Manager, per cui è necessaria la reimpostazione del telefono, il file di configurazione del telefono viene modificato automaticamente.

I file di configurazione contengono inoltre delle informazioni sull'immagine di avvio che dovrebbe essere eseguita sul telefono. Se l'immagine di avvio è diversa da quella attualmente caricata sul telefono, quest'ultimo contatta il server TFTP per richiedere i file di avvio richiesti.

Se in Cisco Unified Communications Manager Administrationvengono configurate delle impostazioni di protezione, il file di configurazione del telefono conterrà delle informazioni riservate. Per garantire la privacy del file di configurazione, è necessario configurarlo per la crittografia. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso. Il telefono richiede un file di configurazione ogni volta che viene reimpostato e registrato su Cisco Unified Communications Manager.

Il telefono accede a un file di configurazione predefinito denominato XmlDefault.cnf.xml sul server TFTP se si verificano le condizioni seguenti:

- È stata abilitata la registrazione automatica in Cisco Unified Communications Manager
- Il telefono non è stato aggiunto al database di Cisco Unified Communications Manager.
- Il telefono viene registrato per la prima volta.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Comportamento del telefono durante le ore di congestione della rete

La qualità audio e video del telefono può essere influenzata da qualsiasi calo delle prestazioni di rete che in alcuni casi potrebbe comportare persino la perdita di una chiamata. I motivi del calo delle prestazioni della rete includono, tra l'altro, le attività seguenti:

- Attività amministrative, come la scansione di una porta interna o l'analisi della sicurezza.
- Attacchi nella rete, come un attacco Denial of Service.

Comportamento del telefono su una rete con due router di rete

Il telefono IP Cisco serie 8800 utilizza un firewall per fornire protezione contro le intrusioni informatiche, come ad esempio attacchi man-in-the-middle. Non è possibile disabilitare questo firewall. Tale firewall arresta il traffico sul telefono se si configura la rete con due router di rete nella stessa subnet e con reindirizzamento IP.

Il firewall del telefono arresta il traffico perché questa impostazione di rete è simile a un attacco man-in-the-middle. Il telefono riceve dei pacchetti di reindirizzamento per diversi IP di destinazione in una subnet diversa dal telefono. Il telefono si trova su una rete con più di un router e il router predefinito invia il traffico a un secondo router.

Controllare i registri del telefono se si sospetta che il firewall stia arrestando il traffico. Cercare la notifica del codice di errore 1 inviata dal sistema operativo quando ha tentato di stabilire una connessione. Una delle firme è

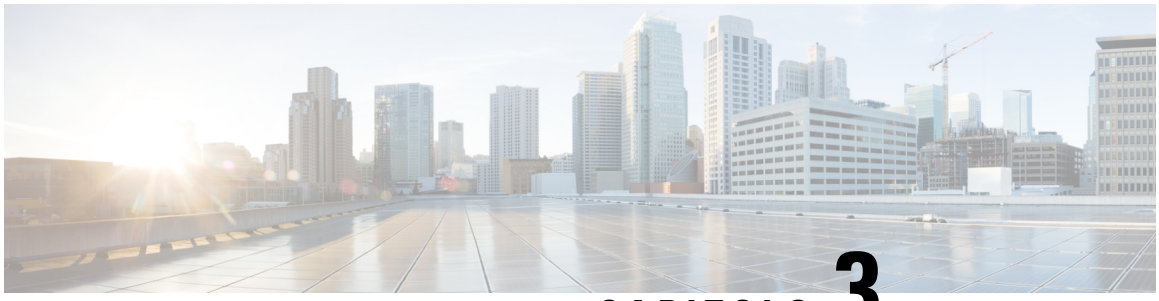
```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Una rete con due router di rete nella stessa subnet e con reindirizzamento IP non corrisponde a una configurazione comune. Se si utilizza questa impostazione di rete, prendere in considerazione l'uso di un solo router su una subnet. Tuttavia, se è necessario utilizzare due router di rete sulla stessa subnet, disabilitare il reindirizzamento IP sul router e riavviare il telefono.

Application Programming Interface

Cisco supporta l'utilizzo di API telefoniche con applicazioni di terze parti testate e certificate tramite Cisco dallo sviluppatore di applicazioni di terze parti. Tutti i problemi del telefono relativi all'interazione dell'applicazione non certificata devono essere risolti dalle terze parti e non verranno affrontati da Cisco.

Per il modello di supporto delle applicazioni/soluzioni Cisco certificate di terze parti, consultare il sito Web di Cisci Solution Partner Program per ulteriori informazioni.



CAPITOLO 3

Hardware del telefono IP Cisco

Panoramica sul telefono

Il telefono IP Cisco serie 8800 offre comunicazione vocale su rete IP (Internet Protocol). Il telefono IP Cisco funziona in modo simile a qualsiasi telefono aziendale digitale, consentendo di effettuare chiamate, nonché di accedere a funzioni come ad esempio la disattivazione dell'audio, la messa in attesa, il trasferimento di chiamata e molto altro. Inoltre, tramite il collegamento alla rete dati, il telefono offre funzioni di telefonia IP migliorate, inclusi l'accesso alle informazioni e ai servizi di rete e funzioni e servizi personalizzabili.

Il telefono IP Cisco 8811 dispone di uno schermo LCD in scala di grigi. I telefoni IP Cisco 8841, 8845, 8851, 8851NR, 8861, 8865 e 8865NR dispongono di uno schermo LCD a colori a 24 bit.

L'aggiunta di funzionalità ai tasti linea è limitata dal numero dei tasti linea disponibili. Non è possibile aggiungere altre funzioni al numero di tasti linea sul telefono.

I telefoni IP Cisco dispongono delle seguenti funzioni:

- Tasti funzione programmabili che supportano fino a 5 linee in modalità linea sessione o fino a 10 linee in modalità linea avanzata
- Capacità video complete (soltanto per i telefoni IP Cisco 8845, 8865 e 8865NR)
- Connettività Gigabit Ethernet.
- Supporto Bluetooth per cuffie wireless (soltanto per i telefoni IP Cisco 8845, 8851, 8861 e 8865. Questa funzione non è supportata sui telefoni IP Cisco 8811, 8841, 8851NR e 8865NR).
- Supporto per microfono e altoparlanti esterni (soltanto per i telefoni IP Cisco 8861, 8865 e 8865NR)
- Connettività di rete tramite Wi-Fi (soltanto per i telefoni IP Cisco 8861 e 8865. Il Wi-Fi non è supportato sul telefono IP Cisco 8865NR).
- Porte USB:

- Una porta USB sui telefoni IP Cisco 8851 e 8851NR
- Due porte USB sui telefoni IP Cisco 8861, 8865 e 8865NR

I telefoni IP Cisco 8845, 8865 e 8865NR supportano le videochiamate grazie alla videocamera incorporata. Utilizzare questa funzione per collaborare con amici e colleghi o per organizzare incontri faccia a faccia tramite telefono.

Nota È necessario conservare la scatola e la confezione del telefono IP Cisco 8845, 8865 e 8865NR. Le videocamere di questi telefoni sono fragili. Se si sposta il telefono, si consiglia di imballare il telefono nella scatola originale per proteggere la videocamera. Per ulteriori informazioni, consultare Protezione della videocamera del telefono, a pagina 39.

Le videochiamate includono le seguenti funzioni:

- PiP: è possibile selezionarla da quattro posizioni: in basso a destra, in alto a destra, in alto a sinistra e in basso a sinistra. È possibile inoltre anche disattivare tale funzione.
- Scambio: attiva o disattiva le visualizzazioni nella vista PiP. La softkey Scambio è disabilitata se PIP è disattivato.
- Video PropriaImmag: selezionare Video PropriaImmag per visualizzare la propria immagine come appare nel video.
- Interfaccia utente video e Iniziazione conferenza/trasferimento: selezionare per avviare una conferenza.

Per ulteriori informazioni sulle videochiamate, consultare la *Guida per l'utente del telefono IP Cisco serie 8800 per Cisco Unified Communications Manager* e la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Come altri dispositivi, è necessario configurare e gestire i telefoni IP Cisco. Tali telefoni effettuano la codifica e la decodifica dei codec seguenti:

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab
- G.726
- iLBC
- Opus
- iSAC

Attenzione L'utilizzo di un telefono cellulare, portatile o GSM oppure di radio con due frequenze in prossimità di un telefono IP Cisco può causare interferenze. Per ulteriori informazioni, fare riferimento alla documentazione del produttore del dispositivo che causa interferenza.

I telefoni IP Cisco forniscono funzionalità di telefonia tradizionali, come trasferimento e inoltro delle chiamate, ripetizione del numero, chiamata rapida, chiamata in conferenza e accesso al sistema di messaggistica vocale. I telefoni IP Cisco forniscono inoltre numerose altre funzioni.

Come con altri dispositivi di rete, è necessario configurare i telefoni IP Cisco per prepararli all'accesso a Cisco Unified Communications Manager e al resto della rete IP. Tramite DHCP, il numero di impostazioni da configurare sul telefono è minore. Se la rete lo richiede, tuttavia, è possibile configurare manualmente informazioni quali indirizzo IP, server TFTP e dati sulla subnet.

I telefoni IP Cisco possono interagire con altri servizi e dispositivi nella rete IP per fornire funzioni migliorate. Ad esempio, è possibile integrare Cisco Unified Communications Manager con la rubrica standard Lightweight Directory Access Protocol 3 (LDAP3) aziendale per consentire agli utenti di cercare le informazioni di contatto dei colleghi direttamente dai loro telefoni IP. È inoltre possibile utilizzare XML per consentire agli utenti di accedere a informazioni come meteo, mercato azionario, quotazioni correnti e altre informazioni basate sul Web.

Infine, poiché il telefono IP Cisco è un dispositivo di rete, è possibile ottenere delle informazioni dettagliate sullo stato. Tali informazioni possono risultare valide per la risoluzione di eventuali problemi riscontrati dagli utenti durante l'utilizzo dei telefoni IP. È inoltre possibile ottenere statistiche su una chiamata attiva o sulle versioni firmware del telefono.

Per poter funzionare nella rete di telefonia IP, il telefono IP Cisco deve essere collegato a un dispositivo di rete, come uno switch Cisco Catalyst. È inoltre necessario registrare il telefono IP Cisco nel sistema Cisco Unified Communications Manager prima di effettuare e ricevere chiamate.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Telefono IP Cisco 8811

Nella sezione riportata di seguito vengono descritti gli attributi di Telefono IP Cisco 8811.

Cisco 8811

Connettere il telefono alla rete di telefonia IP aziendale come mostrato nel diagramma seguente.

1	Porta dell'adattatore CC (CC 48 V).	5	Connessione della porta di accesso (10/100/1000 PC).
2	Alimentatore CA/CC (opzionale).	6	Porta ausiliaria.
3	Spina dell'alimentatore CA (opzionale).	7	Connessione del ricevitore.
4	Connessione della porta di rete (10/100/1000 SW). Alimentazione IEEE 802.3at abilitata.	8	Connessione della cuffia analogica (opzionale).

Nota Telefono IP Cisco 8811 non supporta il modulo di espansione tasti.

Telefoni IP Cisco 8841 e 8845

Nella sezione riportata di seguito vengono descritti gli attributi dei telefoni IP Cisco 8841 e 8845.

Collegamenti del telefono

Connettere il telefono alla rete di telefonia IP aziendale utilizzando il seguente schema.

1	Porta dell'adattatore CC (CC 48 V).	5	Connessione della porta di accesso (10/100/1000 PC).
2	Alimentatore CA/CC (opzionale).	6	Porta ausiliaria.
3	Spina dell'alimentatore CA (opzionale).	7	Connessione del ricevitore.
4	Connessione della porta di rete (10/100/1000 SW). Alimentazione IEEE 802.3at abilitata.	8	Connessione della cuffia analogica (opzionale).

Nota I telefoni IP Cisco 8841 e 8845 non supportano un modulo di espansione tasti.

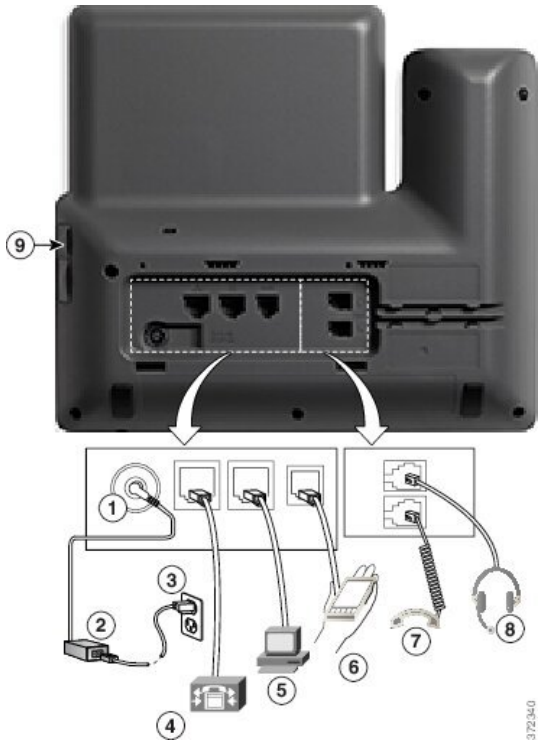
Telefono IP Cisco 8851 e 8851NR

Nella sezione riportata di seguito vengono descritti gli attributi dei telefoni IP Cisco 8851 e 8851NR.

Nota Il telefono IP Cisco 8851NR non supporta il Bluetooth. Invece, i telefoni IP Cisco 8851 e 8851NR supportano le stesse funzioni.

Cisco 8851

Connettere il telefono alla rete di telefonia IP aziendale come mostrato nel diagramma seguente.



1	Porta dell'adattatore CC (CC 48 V).	6	Porta ausiliaria.
2	Alimentatore CA/CC (opzionale).	7	Connessione del ricevitore.
3	Spina dell'alimentatore CA (opzionale).	8	Connessione della cuffia analogica (opzionale).
4	Connessione della porta di rete (10/100/1000 SW). Alimentazione IEEE 802.3at abilitata.	9	Porta USB.
5	Connessione della porta di accesso (10/100/1000 PC).		

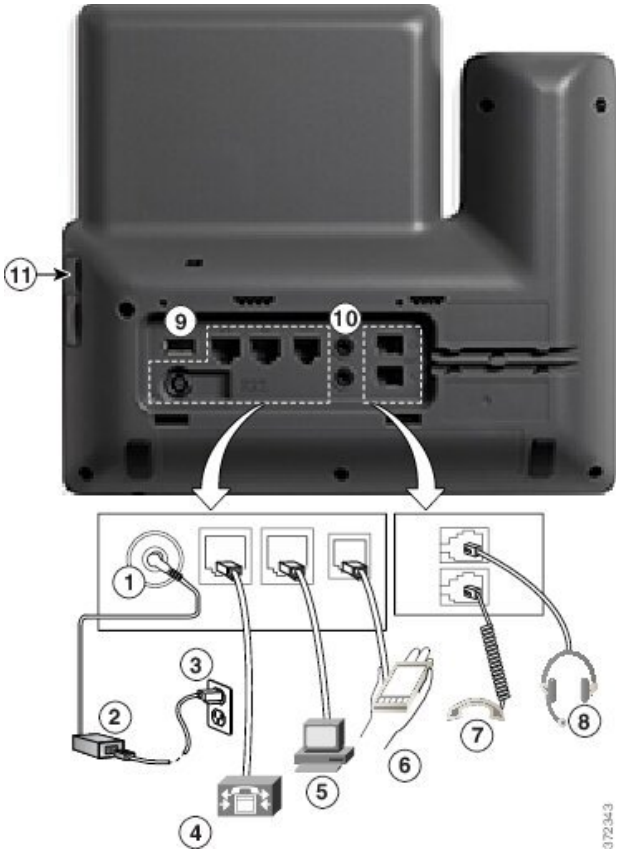
Nota Ciascuna porta USB supporta la connessione di un massimo di cinque dispositivi supportati e non supportati. Ciascun dispositivo collegato al telefono è incluso nel numero massimo di dispositivi. A titolo esemplificativo, il telefono può supportare cinque dispositivi USB sulla porta laterale, ad esempio due moduli di espansione tasti, una cuffia, un hub e un altro dispositivo USB standard. Molti prodotti USB di terze parti contano come più dispositivi USB, ad esempio un dispositivo contenente una cuffia e un hub USB può contare come due dispositivi USB. Per ulteriori informazioni, consultare la documentazione del dispositivo USB.

Telefoni IP Cisco 8861, 8865 e 8865NR

Nella sezione riportata di seguito vengono descritti gli attributi dei telefoni IP Cisco 8861, 8865 e 8865NR.

Collegamenti del telefono

Connettere il telefono alla rete di telefonia IP aziendale come mostrato nel diagramma seguente.



1	Porta dell'adattatore CC (CC 48 V).	7	Connessione del ricevitore.
2	Alimentatore CA/CC (opzionale).	8	Connessione della cuffia analogica (opzionale).
3	Spina dell'alimentatore CA (opzionale).	9	Porta USB.
4	Connessione della porta di rete (10/100/1000 SW). Alimentazione IEEE 802.3at abilitata.	10	Porte audio ingresso/uscita.
5	Connessione della porta di accesso (10/100/1000 PC).	11	Porta USB.
6	Porta ausiliaria.		

Nota Ciascuna porta USB supporta la connessione di un massimo di cinque dispositivi supportati e non supportati. Ciascun dispositivo collegato al telefono è incluso nel numero massimo di dispositivi. A titolo esemplificativo, il telefono può supportare cinque dispositivi USB (ad esempio, tre moduli di espansione tasti, un hub e un altro dispositivo USB standard) sulla porta laterale e cinque dispositivi aggiuntivi USB standard sulla porta posteriore. Molti prodotti USB di terze parti contano come più dispositivi USB, ad esempio un dispositivo contenente una cuffia e un hub USB può contare come due dispositivi USB. Per ulteriori informazioni, consultare la documentazione del dispositivo USB.

Pulsanti e hardware

Il telefono IP Cisco serie 8800 dispone di due distinti tipi di hardware:

- I telefoni IP Cisco 8811, 8841, 8851, 8851NR e 8861: non dispongono di videocamera.
- I telefoni IP Cisco 8845 e 8865 e 8865NR: dispongono di videocamera integrata.

La figura che segue mostra il telefono IP Cisco 8845.

Figura 1: Pulsanti e hardware del telefono IP Cisco 8845

Nella seguente tabella sono descritti i pulsanti del telefono IP Cisco serie 8800.

Tabella 18: Pulsanti del telefono IP Cisco serie 8800

1	Ricevitore e striscia luminosa ricevitore	Indica se c'è una chiamata in arrivo (rosso intermittente) o un nuovo messaggio vocale (rosso fisso).
2	Videocamera Solo telefoni IP Cisco 8845, 8865 e 8865NR	Utilizzare la videocamera per le videochiamate.

3	Tasti funzione programmabili e pulsanti linea	Consentono di accedere alle linee del telefono, a funzioni e sessioni di chiamata. L'aggiunta di funzionalità ai tasti linea è limitata dal numero dei tasti linea disponibili. Non è possibile aggiungere altre funzioni al numero di tasti linea sul telefono. Per ulteriori informazioni, consultare la sezione Softkey, pulsanti linea e funzioni nel capitolo "Hardware del telefono IP Cisco".
4	Pulsanti softkey	Consente di accedere a funzioni e servizi. Per ulteriori informazioni, consultare la sezione Softkey, pulsanti linea e funzioni nel capitolo "Hardware del telefono IP Cisco".
5	**Indietro**, cluster di navigazione e **Rilascia**	**Indietro** Consente di tornare al menu o alla schermata precedente. Cluster di navigazione Pulsante multidirezione e pulsante **Selez.**: consentono di scorrere tra i menu, evidenziare voci e selezionare la voce evidenziata. **Rilascia** Consente di chiudere una chiamata connessa o una sessione.
6	**Attesa/Riprendi**, **Conferenza** e **Trasferisci**	**Attesa/Riprendi** Consente di mettere in attesa una chiamata attiva o di riprendere una chiamata in attesa. **Conferenza** Consente di creare una chiamata in conferenza. **Trasferisci** Consente di trasferire una chiamata.
7	**Altoparlante**, **Disattiva audio** e **Cuffia**	**Altoparlante** Consente di attivare o disattivare l'altoparlante. Quando tale funzionalità è attiva, il pulsante è illuminato. **Disattiva audio** Consente di attivare o disattivare il microfono. Quando il microfono è disattivato, il pulsante è illuminato. **Cuffia** Consente di attivare la cuffia. Quando la cuffia è attivata, il pulsante è accesso. Per uscire dalla modalità Cuffia, sollevare il ricevitore o selezionare **Altoparlante** .
8	**Contatti**, **Applicazioni** e **Messaggi**	**Contatti** Consente di accedere agli elenchi personali e aziendali. **Applicazioni** Consente di accedere alle chiamate recenti, alle preferenze utente, alle impostazioni del telefono e alle informazioni sul modello del telefono. **Messaggi** Consente di accedere al sistema di messaggistica vocale.

9	Pulsante del **volume**	Consente di regolare il volume del ricevitore, della cuffia e dell'altoparlante (ricevitore sganciato) e il volume della suoneria (ricevitore agganciato).

Softkey, pulsanti linea e tasti funzione

È possibile interagire con le funzioni del telefono in vari modi:

- I softkey, sotto lo schermo, consentono di accedere alle funzioni visualizzate sullo schermo sopra il softkey e cambiano in base alle operazioni che si stanno eseguendo al momento. Il softkey **Altro...** indica che sono disponibili altre funzioni.
- I pulsanti linea e i tasti funzione, posizionati sui lati dello schermo, consentono di accedere alle funzioni e alle linee del telefono.
  - Tasti funzione - Utilizzati per funzioni quali **Richiamata rapida** o **Risposta per assente** e per visualizzare lo stato dell'utente su un altra linea.
  - Pulsanti linea: consentono di rispondere a una chiamata o di riprendere una chiamata in attesa. Se non sono utilizzati per una chiamata attiva, consentono di avviare funzioni del telefono, ad esempio la visualizzazione delle chiamate non risposte.

I pulsanti linea e i tasti funzione si accendono per indicare lo stato.

Colore e stato del LED	**Modalità linea normale: pulsanti linea**	**Modalità linea normale: tasti funzione** **Modalità linea avanzata**
LED verde fisso	Chiamata attiva o chiamata bidirezionale, chiamata in attesa, privacy in uso	Chiamata attiva o chiamata bidirezionale, privacy in uso
LED verde lampeggiante	Non applicabile	Chiamata in attesa
LED arancione fisso	Chiamata in arrivo, ripristino di una chiamata, chiamata interna monodirezionale, connessione a un gruppo di ricerca	Chiamata interna monodirezionale, connessione a un gruppo di ricerca
LED arancione lampeggiante	Non applicabile	Chiamata in arrivo, ripresa dall'attesa
LED rosso fisso	Linea remota in uso, linea remota in attesa, Non disturbare attivo	Linea remota in uso, Non disturbare attivo
LED rosso lampeggiante	Non applicabile	Linea remota in attesa

L'amministratore può impostare alcune funzioni come softkey o tasti funzione. È inoltre possibile accedere ad alcune funzioni con i softkey o con i pulsanti fisici associati.

Protezione della videocamera del telefono

La videocamera del telefono è fragile e potrebbe rompersi durante il trasporto del telefono.

Prima di iniziare

È necessario proteggere la videocamera in uno dei seguenti modi:

- Scatola del telefono originale e materiale di imballo
- Materiale di imballo, come schiuma o pluriball

Procedura

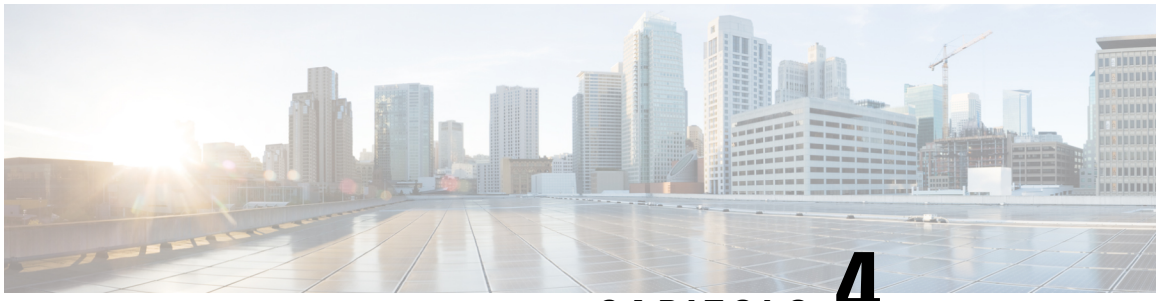
Passaggio 1 Se si dispone della scatola originale:

a) Posizionare la schiuma sulla videocamera in modo tale che l'obiettivo sia ben protetto.
b) Posizionare il telefono nella sua scatola originale.

Passaggio 2 Se non si dispone della casella, avvolgere con cautela il telefono con la schiuma o il Bubble wrap per proteggere la videocamera. Assicurarsi che la schiuma protegga e circondi la videocamera in modo che niente possa premere contro la videocamera da qualsiasi direzione oppure che la videocamera possa essere danneggiata nel trasporto.

PARTE II

Installazione del telefono IP Cisco



CAPITOLO 4

Installazione del telefono IP Cisco

Verifica dell'impostazione di rete

Durante l'implementazione di un nuovo sistema di telefonia IP, per preparare la rete all'uso del servizio di telefonia IP, gli amministratori di sistema e di rete devono effettuare diverse attività di configurazione iniziale. Per informazioni e un elenco di controllo relativi all'impostazione e alla configurazione di una rete di telefonia IP Cisco, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Per garantire un corretto funzionamento del telefono come endpoint nella rete, quest'ultima deve rispettare dei requisiti specifici. Un requisito è la larghezza di banda appropriata. I telefoni richiedono più larghezza di banda rispetto ai 32 kbps consigliati quando vengono registrati su Cisco Unified Communications Manager. Prendere in considerazione questo requisito di larghezza di banda maggiore quando si configura la larghezza di banda di QoS. Per ulteriori informazioni, consultare *Solution Reference Network Design (SRND) di Cisco Collaboration System 12.x* o versioni successive (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html).

Nota Sul telefono vengono visualizzate la data e l'ora da Cisco Unified Communications Manager. L'ora visualizzata sul telefono può essere diversa dall'ora di Cisco Unified Communications Manager fino a un massimo di 10 secondi.

Procedura

Passaggio 1 Configurare una rete VoIP in base ai requisiti seguenti:

- La rete VoIP è configurata sui router e i gateway.
- Cisco Unified Communications Manager è installato nella rete ed è configurato per la gestione dell'elaborazione delle chiamate.

Passaggio 2 Impostare la rete per il supporto di una delle funzioni seguenti:

- Supporto DHCP
- Assegnazione manuale di indirizzo IP, gateway e subnet mask

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Onboarding tramite codice di attivazione per telefoni in sede

È possibile utilizzare l'onboarding tramite codice di attivazione per impostare rapidamente nuovi telefoni senza eseguire la registrazione automatica. Con questo metodo è possibile controllare l'onboarding del telefono in uno dei seguenti modi:

- Strumento BAT (Bulk Administration Tool) di Cisco Unified Communications
- Interfaccia di Cisco Unified Communications Manager Administration
- Servizio Web AXL (Administravie XML)

Abilitare questa funzione dalla sezione **Informazioni dispositivo** della pagina Configurazione telefono. Selezionare **Richiedi codice di attivazione per onboarding** se si desidera applicare questa funzione a un singolo telefono in sede.

Prima di poter effettuare la registrazione, gli utenti devono immettere un codice di attivazione. L'onboarding tramite codice di attivazione è applicabile ai singoli telefoni, a un gruppo di telefoni o a un'intera rete.

È facile per gli utenti eseguire l'onboarding del telefono perché devono solo immettere un codice di attivazione di 16 cifre. I codici vengono immessi manualmente o mediante un codice QR se il telefono dispone di una videocamera. Si consiglia di utilizzare un metodo sicuro per fornire agli utenti queste informazioni. Tuttavia, se un utente viene assegnato a un telefono, queste informazioni sono disponibili nel portale Self Care. Nel registro di controllo viene registrato quando un utente accede al codice dal portale.

I codici di attivazione possono essere utilizzati solo una volta e scadono dopo 1 settimana per impostazione predefinita. Se un codice è scaduto, è necessario fornirne uno nuovo all'utente.

Questo metodo è un modo semplice per proteggere la rete perché non è possibile registrare un telefono finché non vengono verificati il certificato MIC (Manufacturing Installed Certificate) e il codice di attivazione. Questo metodo è inoltre utile per eseguire in blocco l'onboarding dei telefoni perché non utilizza il TAPS (Tool for Auto-Registered Phones Support, Strumento di supporto per la registrazione automatica del telefono) o la registrazione automatica. La velocità dell'onboarding è un telefono al secondo o circa 3600 all'ora. Per

aggiungere i telefoni è possibile utilizzare Cisco Unified Communications Manager Administration, il servizio Web AXL (Administrative XML Web Service) o lo strumento BAT.

Una volta configurati per l'onboarding tramite codice di attivazione, i telefoni vengono reimpostati. Non è possibile eseguire la registrazione finché non viene inserito il codice di attivazione e non viene verificato il certificato MIC del telefono. Prima di implementarla, informare gli utenti del passaggio all'onboarding tramite codice di attivazione.

Per ulteriori informazioni, vedere *Guida all'amministrazione di Cisco Unified Communications Manager e IM e Presence Service, versione 12.0(1)* o versioni successive.

Onboarding tramite codice di attivazione e accesso mobile e remoto

È possibile utilizzare l'onboarding tramite codice di attivazione con l'accesso mobile e remoto quando si distribuiscono i telefoni IP Cisco per gli utenti remoti. Questa funzione è un modo sicuro per distribuire i telefoni fuori sede quando la registrazione automatica non è richiesta. Tuttavia, è possibile configurare la registrazione automatica per telefoni in sede e codici di attivazione per telefoni fuori sede. Questa funzione è simile all'onboarding tramite codice di attivazione per i telefoni in sede, ma rende disponibile il codice di attivazione anche per i telefoni fuori sede.

L'onboarding tramite codice di attivazione per l'accesso mobile e remoto richiede Cisco Unified Communications Manager 12.5(1)SU1 o versioni successive e Cisco Expressway X12.5 o versioni successive. È inoltre possibile abilitare la generazione di licenze smart con Smart Licensing.

È possibile abilitare questa funzione da Cisco Unified Communications Manager Administration, ma tenere presente quanto segue:

- Abilitare questa funzione dalla sezione **Informazioni dispositivo** della pagina Configurazione telefono.
- Selezionare **Richiedi codice di attivazione per onboarding** se si desidera applicare questa funzione solo a un singolo telefono in sede.
- Selezionare **Consenti codice di attivazione tramite MRA** e **Richiedi codice di attivazione per onboarding** se si desidera utilizzare l'onboarding tramite attivazione per un singolo telefono fuori sede. Se il telefono è in sede, passa alla modalità Accesso mobile e remoto e utilizza la Expressway. Se il telefono non è in grado di raggiungere la Expressway, non viene registrato fino a quando non è fuori sede.

Per ulteriori informazioni, consultare i seguenti documenti:

- *Guida all'amministrazione di Cisco Unified Communications Manager e IM e Presence Service, versione 12.0(1)*
- *Accesso mobile e remoto tramite Cisco Expressway* per Cisco Expressway x 12.5 o versioni successive

Abilitazione della registrazione automatica sul telefono

Per la gestione dell'elaborazione delle chiamate sul telefono IP Cisco, è necessario Cisco Unified Communications Manager. Consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso o la guida contestuale in Cisco Unified Communications Manager

Administration per assicurarsi che Cisco Unified Communications Manager sia impostato correttamente per la gestione del telefono e l'indirizzamento e l'elaborazione delle chiamate.

Prima di installare il telefono IP Cisco, è necessario selezionare un metodo per l'aggiunta dei telefoni al database di Cisco Unified Communications Manager.

Abilitando la registrazione automatica prima dell'installazione dei telefoni, è possibile:

- Aggiungere i telefoni senza prima raccogliere i relativi indirizzi MAC.
- Aggiungere automaticamente un telefono IP Cisco al database di Cisco Unified Communications Manager quando lo si connette fisicamente alla rete di telefonia IP. Durante la registrazione automatica, Cisco Unified Communications Manager assegna al telefono il numero di rubrica successivo consecutivo disponibile.
- Immettere rapidamente i telefoni nel database di Cisco Unified Communications Manager e modificare le impostazioni, come ad esempio i numeri di rubrica, da Cisco Unified Communications Manager.
- Spostare i telefoni registrati automaticamente in nuove posizioni e assegnarli a diversi gruppi di dispositivi senza modificare i numeri di rubrica corrispondenti.

La registrazione automatica è disabilitata per impostazione predefinita. In alcuni casi, non è consigliabile utilizzarla; ad esempio, se si desidera assegnare un numero di rubrica specifico al telefono o se si desidera utilizzare una connessione protetta con Cisco Unified Communications Manager. Per informazioni sull'abilitazione della registrazione automatica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso. Se si configura il cluster per la modalità mista tramite il client Cisco CTL, la registrazione automatica viene automaticamente disabilitata. L'utente può comunque abilitarla nuovamente. Se si configura il cluster per la modalità non protetta tramite il client Cisco CTL, la registrazione automatica non viene abilitata automaticamente.

È possibile aggiungere dei telefoni con il processo di registrazione automatica e lo strumento TAPS (Tool for AutoRegistered Phones Support) senza prima raccogliere i relativi indirizzi MAC.

Lo strumento TAPS funziona con lo strumento BAT (Bulk Administration Tool) per l'aggiornamento di un gruppo di telefoni già aggiunti al database di Cisco Unified Communications Manager con indirizzi MAC fittizi. Utilizzare lo strumento TAPS per aggiornare gli indirizzi MAC e scaricare le configurazioni predefinite per i telefoni.

Cisco consiglia di utilizzare la registrazione automatica e lo strumento TAPS per aggiungere meno di 100 telefoni alla rete. Per aggiungere più di 100 telefoni alla rete, utilizzare lo strumento Bulk Administration Tool (BAT).

Per implementare lo strumento TAPS, comporre (o chiedere all'utente finale di farlo) un numero di rubrica TAPS e seguire le istruzioni vocali. Al termine del processo, sul telefono saranno presenti il numero di rubrica e altre impostazioni e il telefono sarà stato aggiornato su Cisco Unified Communications Manager Administration con l'indirizzo MAC corretto.

Prima di connettere il telefono IP Cisco alla rete, verificare che la registrazione automatica sia abilitata e configurata correttamente in Cisco Unified Communications Manager Administration. Per informazioni sull'abilitazione e la configurazione della registrazione automatica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Affinché lo strumento TAPS funzioni, è necessario che la registrazione automatica sia abilitata in Cisco Unified Communications Manager Administration.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, fare clic su **Sistema** > **Cisco Unified CM**.

Passaggio 2 Fare clic su **Trova** e selezionare il server desiderato.

Passaggio 3 In **Informazioni sulla registrazione automatica**, configurare i seguenti campi.

- **Modello dispositivo universale**
- **Modello di linea universale**
- **Numero di rubrica iniziale**
- **Numero di rubrica finale**

Passaggio 4 Deselezionare la casella di controllo **Registrazione automatica disabilitata su questo Cisco Unified Communications Manager**.

Passaggio 5 Fare clic su **Salva**.

Passaggio 6 Fare clic su **Applica configurazione**.

Installazione del telefono IP Cisco

Dopo aver collegato il telefono alla rete, inizia il processo di avvio e il telefono viene registrato in Cisco Unified Communications Manager. Per terminare l'installazione del telefono, configurare le impostazioni di rete sul telefono a seconda che si abiliti o disabiliti il servizio DHCP.

Se si utilizza la registrazione automatica, è necessario aggiornare le informazioni sulla configurazione specifiche del telefono come l'associazione del telefono a un utente, la modifica della tabella dei pulsanti o il numero di rubrica.

Nota Prima di utilizzare dispositivi esterni, consultare Dispositivi esterni, a pagina 26.

Per informazioni sull'installazione degli accessori, consultare *Guida agli accessori del telefono IP Cisco serie 7800 e 8800 per Cisco Unified Communications Manager*.

Se la scrivania è dotata di un solo cavo LAN, è possibile collegare il telefono alla LAN tramite la porta SW e collegare il computer alla porta PC. Per ulteriori informazioni, consultare Condivisione della connessione di rete con il telefono e il computer, a pagina 49.

È inoltre possibile collegare in cascata i due telefoni. Collegare la porta PC del primo telefono alla porta SW del secondo telefono.

Attenzione Non collegare le porte PC e SW alla LAN.

Procedura

Passaggio 1 Scegliere la fonte di alimentazione per il telefono:

- PoE (Power over Ethernet)
- Alimentazione esterna

Per ulteriori informazioni, consultare Requisiti di alimentazione dei telefoni, a pagina 16.

Passaggio 2 Collegare il ricevitore all'apposita porta e premere il cavo nel relativo canale del telefono.

Il ricevitore wideband compatibile è progettato specificatamente per l'uso con il telefono IP Cisco. Sul ricevitore è presente una striscia luminosa che indica le chiamate in arrivo e la presenza di messaggi vocali in attesa.

Attenzione Se non si inserisce il cavo nel canale, i circuito stampato potrebbe danneggiarsi. Il canale del cavo riduce la tensione sul connettore e sul circuito stampato.

Passaggio 3 Collegare una cuffia o una cuffia wireless. È possibile aggiungere una cuffia in seguito se non viene collegata subito.

Premere il cavo nel relativo canale.

Attenzione Se non si inserisce il cavo nel canale, i circuito stampato del telefono potrebbe danneggiarsi. Il canale del cavo riduce la tensione sul connettore e sul circuito stampato.

Passaggio 4 Collegare un cavo diritto Ethernet dalla porta dello switch alla porta di rete con etichetta 10/100/1000 SW sul telefono IP Cisco. Ogni telefono IP Cisco è fornito di un cavo Ethernet in dotazione.

Utilizzare cavi di categoria 3, 5, 5e o 6 per le connessioni 10 Mbps, di categoria 5, 5e o 6 per le connessioni 100 Mbps e di categoria 5e o 6 per connessioni 1000 Mbps. Per ulteriori informazioni, consultare Disposizione dei pin delle porte di rete e computer, a pagina 14 per le linee guida.

Passaggio 5 Collegare un cavo Ethernet diritto da un altro dispositivo di rete, ad esempio un computer desktop, alla porta computer sul telefono IP Cisco. È possibile collegare un altro dispositivo di rete in seguito, se non ne viene collegato uno subito.

Utilizzare cavi di categoria 3, 5, 5e o 6 per le connessioni 10 Mbps, di categoria 5, 5e o 6 per le connessioni 100 Mbps e di categoria 5e o 6 per connessioni 1000 Mbps. Per ulteriori informazioni, consultare Disposizione dei pin delle porte di rete e computer, a pagina 14 per le linee guida.

Passaggio 6 Se il telefono è sulla scrivania, regolare il supporto. Con un telefono montato a parete, potrebbe essere necessario regolare il supporto del ricevitore in modo che non scivoli fuori dal relativo alloggiamento.

Passaggio 7 Monitorare il processo di avvio del telefono. Tramite questo passaggio, è possibile aggiungere al telefono dei numeri di rubrica primari e secondari e delle funzioni associate a tali numeri di rubrica, nonché verificare che il telefono sia configurato correttamente.

Passaggio 8 Se si configurano le impostazioni di rete sul telefono, è possibile impostare un indirizzo IP per il telefono tramite DHCP o specificando manualmente un indirizzo IP.

Consultare Configurazione delle impostazioni di rete, a pagina 59 e Impostazione di rete, a pagina 241.

Passaggio 9 Aggiornare il telefono all'immagine firmware corrente.

Gli aggiornamenti del firmware sull'interfaccia WLAN possono richiedere più tempo rispetto a un'interfaccia cablata, in base alla qualità e alla larghezza di banda della connessione wireless. Alcuni aggiornamenti possono richiedere oltre un'ora.

Passaggio 10 Effettuare chiamate con il telefono IP Cisco per verificare che telefono e funzionalità siano correttamente operativi.

Consultare la *Guida per l'utente del telefono IP Cisco serie 8800*.

Passaggio 11 Fornire informazioni agli utenti finali su come utilizzare i telefoni e configurare le relative opzioni. Questo passaggio assicura che gli utenti dispongano delle informazioni adeguate per utilizzare correttamente i telefoni IP Cisco.

Condivisione della connessione di rete con il telefono e il computer

Per funzionare, è necessario che sia il telefono che il computer si connettano alla rete. Se si dispone di una sola porta Ethernet, i dispositivi possono condividere la connessione di rete.

Prima di iniziare

Prima di poterlo utilizzare, l'amministratore deve abilitare la porta PC in Cisco Unified Communications Manager.

Procedura

Passaggio 1 Collegare la porta SW del telefono alla LAN tramite un cavo Ethernet.

Passaggio 2 Collegare il computer alla porta PC del telefono con un cavo Ethernet.

Impostazione del telefono dai menu di configurazione

Il telefono IP Cisco include i menu di configurazione seguenti:

- Impostazione di rete: fornisce le opzioni per la visualizzazione e la configurazione delle impostazioni di rete come solo IPv4, solo IPv6, WLAN ed Ethernet.
- Impostazione Ethernet: gli elementi di questo menu secondario forniscono delle opzioni per la configurazione del telefono IP Cisco su una rete Ethernet.
- Impostazione client Wi-Fi: gli elementi di questo menu secondario forniscono delle opzioni per la configurazione del telefono IP Cisco su una rete WLAN (Wireless Local Area Network). Il Wi-Fi è supportato solo sul telefono IP Cisco 8861 e 8865.

Nota La porta per PC del telefono è disabilitata quando sul telefono viene abilitato Wi-Fi.

- Impostazione IPv4 e Impostazione IPv6: questi menu secondari dei menu Impostazione Ethernet e Impostazione client Wi-Fi forniscono opzioni di rete aggiuntive.
- Impostazione protezione: fornisce le opzioni per la visualizzazione e la configurazione delle impostazioni di protezione come la modalità di protezione, la Trust List e l'autenticazione 802.1X.

Prima che sia possibile modificare le impostazioni dell'opzione nel menu Impostazione di rete, è necessario sbloccare le opzioni di modifica.

Nota È possibile controllare se un telefono dispone dell'accesso al menu delle impostazioni o alle relative opzioni tramite il campo Accesso alle impostazioni nella finestra Configurazione telefono di Cisco Unified Communications Manager Administration. Il campo Accesso alle impostazioni accetta i valori seguenti:

- Enabled: consente l'accesso al menu delle impostazioni.
- Disabilitato: impedisce l'accesso al menu delle impostazioni.
- Ristretto: consente l'accesso al menu Preferenze utente e di salvare le modifiche del volume. Impedisce l'accesso alle altre opzioni del menu delle impostazioni.

Se non è possibile accedere a un'opzione del menu Impostazioni amministratore, controllare il campo Accesso alle impostazioni.

Procedura

Passaggio 1 Premere **Applicazioni**.

Passaggio 2 Selezionare **Impostazioni amministratore**.

Passaggio 3 Selezionare **Impostazione di rete** o **Impostazione protezione**.

Passaggio 4 Immettere il proprio ID utente e la password, quindi fare clic su **Accedi**.

Passaggio 5 Per visualizzare il menu desiderato, eseguire una di queste azioni:

- Utilizzare le frecce di navigazione per selezionare il menu desiderato e premere **Seleziona**.
- Utilizzare la tastiera del telefono per immettere il numero corrispondente al menu.

Passaggio 6 Per visualizzare un sottomenu, ripetere il passaggio 5.

Passaggio 7 Per uscire da un menu, premere **Esci** o la freccia indietro.

Applicazione di una password al telefono

È possibile applicare una password al telefono. In tal caso, non è possibile apportare modifiche alle opzioni di amministrazione del telefono senza immettere la password nella schermata del telefono Impostazioni amministratore.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, accedere alla finestra Configurazione profilo telefono comune tramite (**Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**).
Passaggio 2	Immettere una password nell'opzione Password di sblocco telefono locale.
Passaggio 3	Applicare la password al profilo del telefono comune utilizzato dal telefono.

Voce di menu e di testo del telefono

Durante la modifica del valore relativo all'impostazione di un'opzione, seguire le linee guida seguenti:

- Utilizzare le frecce sul riquadro di navigazione per evidenziare il campo che si desidera modificare, quindi premere **Seleziona** nel riquadro di navigazione per attivare il campo. Dopo aver attivato il campo, è possibile immettere i valori.
- Utilizzare i tasti della tastiera per immettere i numeri e le lettere.
- Per immettere le lettere con la tastiera, utilizzare il tasto numerico corrispondente. Premere il tasto una o più volte per visualizzare una determinata lettera. Ad esempio, premere il tasto **2** una volta per la «a,» due volte rapidamente per la «b» e tre volte rapidamente per la «c.» Se si effettua una pausa, il cursore avanza automaticamente per consentire l'immissione della lettera successiva.
- In caso di errore, premere la softkey freccia ↩, che consente di eliminare il carattere alla sinistra del cursore.
- Premere **Annulla** prima di premere **Salva** per ignorare le modifiche apportate.
- Per immettere un indirizzo IP, inserire i valori in quattro segmenti già suddivisi. Dopo aver immesso le cifre più a sinistra precedenti al primo periodo, utilizzare il tasto freccia destra per passare al segmento successivo. Il periodo che segue le cifre più a sinistra viene inserito automaticamente.
- Per immettere una virgola in un indirizzo IPv6, premere ***** sulla tastiera.

Nota Se necessario, sul telefono IP Cisco sono disponibili diversi metodi per reimpostare o ripristinare le impostazioni delle opzioni.

Argomenti correlati

Reimpostazione di base, a pagina 277
Applicazione di una password al telefono, a pagina 50

Abilitazione della LAN wireless sul telefono

Prima di impostare una LAN wireless, verificare che il telefono supporti l'uso del wireless. I telefoni IP Cisco 8861 e 8865 supportano una distribuzione LAN wireless. Il telefono IP Cisco 8865NR non supporta la LAN wireless.

Assicurarsi che la copertura Wi-Fi nella posizione in cui viene distribuita la LAN wireless sia adatta per il trasferimento dei pacchetti voce.

Se la connettività Wi-Fi è stata abilitata per la voce e si utilizza la modalità di protezione EAP-FAST o PEAP, autenticare la rete Wi-Fi con l'applicazione Accesso WLAN. Le modalità di protezione aperte e WEP e PSK effettuano l'autenticazione sulla rete Wi-Fi.

Per gli utenti Wi-Fi si consiglia un metodo di roaming veloce e protetto.

Nota La porta per PC del telefono è disabilitata quando sul telefono viene abilitato Wi-Fi.

Per informazioni complete sulla configurazione, consultare la *Guida alla distribuzione della LAN wireless per il telefono IP Cisco 8800* alla posizione seguente:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

La *Guida alla distribuzione della LAN wireless per il telefono IP Cisco 8800* include le informazioni sulla configurazione seguenti:

- Configurazione della rete wireless
- Configurazione della rete wireless in Cisco Unified Communications Manager Administration
- Configurazione della rete wireless sul telefono IP Cisco

Prima di iniziare

Assicurarsi che il Wi-Fi sia abilitato sul telefono e che il cavo Ethernet sia scollegato.

Procedura

Passaggio 1 Per abilitare l'applicazione, premere **Applicazioni**.

Passaggio 2 Accedere a **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione client Wi-Fi** > **Nome di rete**.
Viene visualizzato un elenco dei punti di accesso wireless disponibili ai quali è possibile connettersi.

Passaggio 3 Abilitare la rete wireless.

Impostazione della LAN wireless da Cisco Unified Communications Manager

In Cisco Unified Communications Manager Administration, è necessario abilitare un parametro denominato «Wi-Fi» per il telefono IP wireless Cisco.

Nota Nella finestra Configurazione telefono in Cisco Unified Communications Manager Administration (**Dispositivo** > **Telefono**), utilizzare l'indirizzo MAC della linea cablata durante la configurazione dell'indirizzo MAC. Per la registrazione su Cisco Unified Communications Manager non viene utilizzato l'indirizzo MAC wireless.

Attenersi alla procedura seguente in Cisco Unified Communications Manager Administration.

Procedura

Passaggio 1 Per abilitare la LAN wireless su un telefono specifico, attenersi alla procedura seguente:

a) Selezionare **Dispositivo** > **Telefono**.
b) Individuare il telefono desiderato.
c) Selezionare l'impostazione **Abilitato** per il parametro Wi-Fi nella sezione Layout configurazione specifica del prodotto.
d) Selezionare la casella di controllo **Sovrascrivi impostazioni comuni**.

Passaggio 2 Per abilitare la LAN wireless per un gruppo di telefoni:

a) Selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**.
b) Selezionare l'impostazione **Abilitato** per il parametro Wi-Fi.

Nota Per garantire il corretto funzionamento della configurazione in questa fase, deselezionare la casella di controllo **Sovrascrivi impostazioni comuni** indicata nel passaggio 1d.

c) Selezionare la casella di controllo **Sovrascrivi impostazioni comuni**.
d) Associare i telefoni al profilo telefono comune desiderato tramite le opzioni **Dispositivo** > **Telefono**.

Passaggio 3 Per abilitare la LAN wireless per tutti i telefoni abilitati per la WLAN nella rete:

a) Selezionare **Sistema** > **Configurazione telefono aziendale**.
b) Selezionare l'impostazione **Abilitato** per il parametro Wi-Fi.

Nota Per garantire il corretto funzionamento della configurazione in questa fase, deselezionare la casella di controllo **Sovrascrivi impostazioni comuni** indicata nei passaggi 1d e 2c.

c) Selezionare la casella di controllo **Sovrascrivi impostazioni comuni**.

Impostazione della LAN Wireless dal telefono

Prima che il telefono IP Cisco possa connettersi alla WLAN, è necessario configurare il profilo di rete del telefono con le impostazioni WLAN appropriate. È possibile utilizzare il menu **Impostazione di rete** del telefono per accedere al menu secondario **Impostazione client Wi-Fi** e impostare la configurazione WLAN.

Nota La porta per PC del telefono è disabilitata quando sul telefono viene abilitato Wi-Fi.

Nota L'opzione **Impostazione client Wi-Fi** non viene visualizzata nel menu **Impostazione di rete** se il Wi-Fi è disabilitato su Cisco Unified Communications Manager.

Per ulteriori informazioni, consultare la *Guida alla distribuzione della WLAN del telefono IP Cisco serie 8800*, disponibile qui: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html.

Il campo **Modificabile dall'utente** nel profilo LAN wireless controlla la possibilità di configurare le modalità di protezione sul telefono. Se un utente non può modificare alcuni campi, i campi vengono visualizzati in grigio.

Prima di iniziare

Configurare la LAN wireless da Cisco Unified Communications Manager.

Procedura

Passaggio 1 Premere **Applicazioni**.

Passaggio 2 Selezionare **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione client Wi-Fi**.

Passaggio 3 Impostare la configurazione wireless come descritto nella tabella seguente.

Tabella 19: Opzioni del menu Impostazione client Wi-Fi

Opzione	Descrizione	Per modificare
Nome rete	Specifica il Service Set Identifier, un identificativo univoco per l'accesso ai punti di accesso wireless. Viene visualizzato un elenco dei punti di accesso wireless disponibili.	Consultare Configurazione delle impo rete, a pagina 59.
Impostazione solo IPv4	Nel menu secondario di configurazione Impostazione IPv4, è possibile effettuare le operazioni seguenti: • Abilitare o disabilitare sul telefono l'uso dell'indirizzo IP assegnato dal server DHCP. • Impostare manualmente l'indirizzo IP, la subnet mask, i router predefiniti, il server DNS e i server TFTP alternativi. Per ulteriori informazioni sui campi dell'indirizzo IPv4, consultare Campi di IPv4, a pagina 61.	Scorrere fino all'opzione Impostazion premere **Seleziona**.

Opzione	Descrizione	Per modificare
Impostazione solo IPv6	Nel menu secondario di configurazione Impostazione IPv6, è possibile effettuare le operazioni seguenti: • Abilitare o disabilitare sul telefono l'uso dell'indirizzo IPv6 assegnato dal server DHCPv6 o acquisito tramite la configurazione automatica SLAAC mediante un router abilitato per IPv6. • Impostare manualmente l'indirizzo IPv6, la lunghezza del prefisso, i router predefiniti, il server DNS e i server TFTP alternativi. Per ulteriori informazioni sui campi dell'indirizzo IPv6, consultare Campi di IPv6, a pagina 63.	Scorrere fino all'opzione Impostaz premere **Seleziona**.
Indirizzo MAC	Indirizzo MAC (Media Access Control) univoco del telefono.	Solo visualizzazione. Impossibile
Nome dominio	Nome del dominio DNS (Domain Name System) in cui risiede il telefono.	Consultare Configurazione delle in rete, a pagina 59.

Passaggio 4 Premere **Salva** per apportare le modifiche o premere **Ripristina** per ignorare la connessione.

Impostazione del numero di tentativi di autenticazione WLAN

Una richiesta di autenticazione è una conferma delle credenziali di accesso dell'utente. Si verifica ogni volta che un telefono già collegato a una rete Wi-Fi tenta di riconnettersi al server Wi-Fi, ad esempio in caso di timeout di una sessione Wi-Fi o quando una connessione Wi-Fi viene persa e poi riacquisita.

È possibile configurare il numero di volte che un telefono Wi-Fi invia una richiesta di autenticazione al server Wi-Fi. Il numero di tentativi predefinito è 2, ma è possibile impostare questo parametro da 1 a 3. In caso di mancata l'autenticazione del telefono, all'utente viene richiesto di eseguire nuovamente l'accesso.

È possibile applicare tentativi di autenticazione WLAN a singoli telefoni, a un gruppo di telefoni o a tutti i telefoni Wi-Fi nella rete.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono** e individuare il telefono.

Passaggio 2 Accedere all'area Configurazione specifica del prodotto e impostare il campo **Tentativi di autenticazione WLAN**.

Passaggio 3 Selezionare **Salva**.

Passaggio 4 Selezionare **Applica configurazione**.

Passaggio 5 Riavviare il telefono.

Abilitazione della modalità prompt WLAN

Abilitare la Modalità prompt profilo 1 WLAN se si desidera che un utente esegua l'accesso alla rete Wi-Fi quando accende o reimposta il telefono.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.
Passaggio 2	Individuare il telefono da impostare.
Passaggio 3	Selezionare l'area Configurazione specifica del prodotto e impostare il campo **Modalità prompt profilo 1 WLAN** su **Abilita**.
Passaggio 4	Selezionare **Salva**.
Passaggio 5	Selezionare **Applica configurazione**.
Passaggio 6	Riavviare il telefono.

Impostazione di un profilo Wi-Fi utilizzando Cisco Unified Communications Manager

È possibile configurare un profilo Wi-Fi e successivamente assegnarlo ai telefoni che supportano il Wi-Fi. Il profilo contiene i parametri necessari per connettere i telefoni a Cisco Unified Communications Manager con il Wi-Fi. Quando si crea e si utilizza un profilo Wi-Fi, non è necessario configurare la rete wireless per i singoli telefoni.

I profili Wi-Fi sono supportati su Cisco Unified Communications Manager versione 10.5(2) o versioni successive. EAP-FAST, PEAP-GTC e PEAP-MSCHAPv2 sono supportati in Cisco Unified Communications Manager Release 10.0 e versioni successive. Opus è supportato su Cisco Unified Communications Manager 11.0 e versioni successive.

Un profilo Wi-Fi consente di impedire o limitare le modifiche alla configurazione Wi-Fi del telefono da parte dell'utente.

Quando si utilizza un profilo Wi-Fi, consiglia di utilizzare un profilo di protezione con crittografia TFTP abilitata per proteggere le chiavi e le password.

Se i telefoni sono configurati in modo da utilizzare l'autenticazione EAP-FAST, PEAP-MSCHAPVv2 o PEAP-GTC, gli utenti devono disporre di ID utente e password per eseguire l'accesso al telefono.

I telefoni supportano solo un certificato del server che può essere installato con SCEP o con il metodo di installazione manuale, ma non con entrambi i metodi. I tlefoni non supportano il metodo TFTP per l'installazione del certificato.

Nota I telefoni che utilizzano accesso mobile e remoto tramite Expressway per la connessione a Cisco Unified Communications Manager non possono utilizzare il profilo Wi-Fi. Poiché non si dispone dell'SSID, della modalità di autenticazione e delle credenziali di accesso del telefono dell'utente, non è possibile configurare un profilo LAN wireless per il proprio telefono.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo LAN wireless**.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Passaggio 3 Nella sezione **Informazioni sul profilo LAN wireless**, impostare i parametri:

- **Nome**: immettere un nome univoco per il profilo Wi-Fi. Il nome viene visualizzato sul telefono.
- **Descrizione**: immettere una descrizione per il profilo Wi-Fi per consentire di distinguere questo profilo da altri profili Wi-Fi.
- **Modificabile dall'utente**: selezionare un'opzione:
  - **Consentito**: indica che l'utente può apportare modifiche alle impostazioni Wi-Fi dal proprio telefono. Questa opzione è selezionata per impostazione predefinita.
  - **Non consentito**: indica che l'utente non può apportare modifiche alle impostazioni Wi-Fi sul proprio telefono.
  - **Limitato**: indica che l'utente può modificare il nome utente Wi-Fi e la password sul telefono. Tuttavia, non può apportare modifiche alle altre impostazioni Wi-Fi sul telefono.

Passaggio 4 Nella sezione **Informazioni wireless**, impostare i parametri:

- **SSID (nome di rete)**: immettere il nome di rete disponibile nell'ambiente dell'utente a cui è possibile connettere il telefono. Questo nome viene visualizzato sotto l'elenco delle rete disponibili sul telefono e il telefono può connettersi a questa rete wireless.
- **Banda di frequenza**: le opzioni disponibili sono Automatico, 2,4 GHz e 5 GHz. Questo campo determina la banda di frequenza utilizzata dalla connessione wireless. Se si seleziona Automatico, il telefono tenta di utilizzare per prima la banda a 5 GHz e utilizza la banda a 2,4 GHz solo se quella a 5 GHz non è disponibile.

Passaggio 5 Nella sezione **Impostazioni autenticazioni**, impostare il **Metodo di autenticazione** su uno dei seguenti: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, PSK, WEP e Nessuno.

Una volta impostato questo campo, potrebbero essere visualizzati altri campi da impostare.

- **Certificato utente**: richiesto per l'autenticazione EAP-TLS. Selezionare **Installato dal produttore** o **Installato dall'utente**. Il telefono richiede l'installazione di un certificato, automaticamente nel protocollo SCEP o manualmente nella pagina di amministrazione sul telefono.
- **Passphrase PSK**: richiesta per l'autenticazione PSK. Immettere da 8 a 63 caratteri per la passphrase in formato ASCII o 64 caratteri per quella in formato esadecimale.
- **Chiave WEP**: richiesta per l'autenticazione WEP. Immettere la chiave WEP 40/102 o 64/128 ASCII o esadecimale.
  - 40/104 ASCII è 5 caratteri.
  - 64/128 ASCII è 13 caratteri.
  - 40/104 ESA è 10 caratteri.
  - 64/128 ESA è 26 caratteri.

- **Fornisci credenziali condivise**: richiesto per l'autenticazione EAP-FAST, PEAP-MSCHAPv2 e PEAP-GTC.
  - Se l'utente gestisce il nome utente e la password, lasciare i campi **Nome utente** e **Password** vuoti.
  - Se tutti gli utenti condividono lo stesso nome utente e la stessa password, è possibile immettere le informazioni nei campi **Nome utente** e **Password**.
  - Immettere una descrizione nel campo **Descrizione password**.

Nota Se è necessario assegnare a ciascun utente un nome univoco utente e una password, è necessario creare un profilo per ciascun utente.

Nota Il campo **Profilo di accesso alla rete** non è supportato dal telefono IP Cisco 8861 e 8865.

Passaggio 6 Fare clic su **Salva**.

Operazioni successive

Applicare il gruppo del profilo WLAN a un gruppo di dispositivi (**Sistema** > **Gruppo dispositivi**) o direttamente al telefono (**Dispositivo** > **Telefono**).

Impostazione di un gruppo Wi-Fi utilizzando Cisco Unified Communications Manager

È possibile creare un gruppo di profili LAN wireless e aggiungere qualsiasi profilo LAN wireless a questo gruppo. È possibile assegnare al telefono il gruppo di profili durante la configurazione del telefono.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Gruppo di profili LAN wireless**.

È inoltre possibile definire un gruppo di profili LAN wireless in **Sistema** > **Gruppo dispositivi**.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Passaggio 3 Nella sezione **Informazioni su gruppo di profili LAN wireless**, immettere un nome del gruppo e la relativa descrizione.

Passaggio 4 Nella sezione **Profili per questo gruppo di profili LAN wireless**, selezionare un profilo disponibile dall'elenco **Profili disponibili** e spostare il profilo selezionato nell'elenco **Profili selezionati**.

Se è selezionato più di un profilo LAN wireless, il telefono utilizza solo il primo.

Passaggio 5 Fare clic su **Salva**.

Configurazione delle impostazioni di rete

Procedura

Passaggio 1	Premere **Applicazioni** .
Passaggio 2	Per accedere al menu Impostazioni di rete, selezionare **Impostazioni amministratore** > **Impostazione Ethernet**.
Passaggio 3	Impostare i campi come descritto in Campi di Impostazione Ethernet, a pagina 59.
Passaggio 4	Una volta impostati, selezionare **Applica** e **Salva**.
Passaggio 5	Riavvia il telefono.

Campi di Impostazione Ethernet

Il menu Impostazione di rete contiene i campi e i menu secondari per IPv4 e IPv6. Per modificare alcuni campi, disabilitare innanzitutto il protocollo DHCP.

Se viene stabilita una connessione VPN, i campi dei dati Ethernet verranno sovrascritti.

Tabella 20: Opzioni del menu Impostazione Ethernet

Voce	Tipo	Descrizione
Impostazione IPv4	Menu	Vedere la sezione Campi di IPv4. Questa opzione viene visualizzata soltanto se il telefono è configurato modalità IPv4 e IPv6.
Impostazione IPv6	Menu	Vedere la sezione "Campi di IPv6".
Indirizzo MAC	Stringa	Indirizzo MAC (Media Access Control) univoco del telefono. Solo visualizzazione. Impossibile configurare.
Nome dominio	Stringa	Nome del dominio DNS (Domain Name System) in cui risiede il tele Per modificare questo campo, disattivare il protocollo DHCP.
ID VLAN operativa		VLAN (Virtual Local Area Network) ausiliaria configurata su uno sw appartiene il telefono. Questa impostazione è vuota se non è configurata né la VLAN ausiliaria Se il telefono non ha ricevuto una VLAN ausiliaria, questa opzione indic Se è abilitato il protocollo CDP (Cisco Discovery Protocol) o il protoc Discovery Protocol Media Endpoint Discovery), il telefono non eredi VLAN di amministrazione. Per assegnare un ID VLAN manualmente, utilizzare l'opzione ID VL

Voce	Tipo	Descrizione
ID VLAN amministrazione		VLAN ausiliaria a cui appartiene il telefono. Utilizzata soltanto se il telefono non ha ricevuto una VLAN ausiliaria dall questo valore viene ignorato.
VLAN PC		Consente al telefono di interagire con gli switch di terze parti che non supp Prima che sia possibile modificare questa opzione, è necessario impostar amministrazione.
Impostazione porta SW	Negoziazione automatica 1000 Full 100 Half 10 Half 10 Full	Velocità e duplex della porta di rete. I valori validi specificano: • Negoziazione automatica (impostazione predefinita) • 1000 Full:1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex Se il telefono è connesso a uno switch, configurare la porta dello switch s telefono oppure configurare entrambi sulla negoziazione automatica. Per modificare questa impostazione, sbloccare le opzioni di configurazion di questa opzione viene modificata, è necessario impostare l'opzione Con stesso valore.
Impostazione porta PC	Negoziazione automatica 1000 Full 100 Half 10 Half 10 Full	Velocità e duplex della porta (di accesso) del computer. Valori validi: • Negoziazione automatica (impostazione predefinita) • 1000 Full: 1000-BaseT/full duplex • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex Se il telefono è connesso a uno switch, configurare la porta sullo switch s telefono oppure configurare entrambi sulla negoziazione automatica. Per modificare questo campo, sbloccare le opzioni di configurazione di r impostazione, è necessario impostare l'opzione Configurazione porta SW Per configurare l'impostazione su più telefoni contemporaneamente, attiv remota nella finestra Configurazione telefono aziendale (**Sistema** > **Conf aziendale**). Se le porte sono configurate per la configurazione della porta remota in Cisc Manager Administration, i dati non possono essere modificati sul telefon

Campi di IPv4

Tabella 21: Opzioni del menu Impostazione IPv4

Voce	Descrizione
DHCP abilitato	Indica se il protocollo DHCP è abilitato o disabilitato sul telefono. Se il protocollo DHCP è abilitato, il server DHCP assegna al telefono un indirizzo IP. Se il protocollo DHCP è disabilitato, l'amministratore deve assegnare manualmente un indirizzo IP al telefono. Per ulteriori informazioni, vedere Impostazione del telefono per l'uso del server DHCP, a pagina 65 e Impostazione del telefono sull'utilizzo di un server diverso da DHCP, a pagina 65.
Indirizzo IP	Indirizzo IP (Internet Protocol) del telefono. Se viene utilizzata questa opzione per assegnare un indirizzo IP, è necessario inoltre assegnare una subnet mask e un router predefinito. Osservare le opzioni Subnet mask e Router predefinito in questa tabella.
Subnet mask	La subnet mask utilizzata dal telefono.
Router predefinito	Il router predefinito utilizzato dal telefono.
Server DNS 1 Server DNS 2 Server DNS 3	Server DNS (Domain Name System) primario (Server DNS 1) e server DNS opzionali di backup (Server DNS 2 e 3) utilizzati dal telefono.
TFTP alternativo	Indica se il telefono utilizza un server TFTP alternativo.

Voce	Descrizione
Server TFTP 1	Server TFTP (Trivial File Transfer Protocol) primario utilizzato dal telefono. Se nella rete non viene utilizzato il protocollo DHCP e si desidera modificare tale server, occorre utilizzare l'opzione Server TFTP 1. Se l'opzione TFTP alternativo viene impostata su On, è necessario immettere un valore diverso da zero per l'opzione Server TFTP 1. Se sul file CTL o ITL del telefono non viene elencato né il server TFTP primario né il server TFTP di backup, è necessario sbloccare il file prima di salvare le modifiche all'opzione Server TFTP 1. In questo caso, il telefono elimina il file quando vengono salvate le modifiche all'opzione Server TFTP 1. Un nuovo file CTL o ITL viene scaricato dal nuovo indirizzo del server TFTP 1. Durante la ricerca del server TFTP, il telefono assegna la precedenza ai server TFTP assegnati manualmente a prescindere dal protocollo. Se nella configurazione sono inclusi i server TFTP IPv6 e IPv4, il telefono segue la priorità in base all'ordine di ricerca del server TFTP assegnando la priorità ai server TFTP IPv6 e ai server TFTP IPv4 assegnati manualmente. Il telefono cerca il server TFTP nell'ordine seguente: **1.** Server TFTP IPv4 assegnati manualmente **2.** Server IPv6 assegnati manualmente **3.** Server TFTP assegnati tramite DHCP **4.** Server TFTP assegnati tramite DHCPv6 **Nota** Per informazioni sui file CTL e ITL, consultare la *Guida alla protezione di Cisco Unified Communications Manager*.

Voce	Descrizione
Server TFTP 2	Il server TFTP di backup opzionale utilizzato dal telefono se il server TFTP primario non è disponibile. Se sul file CTL o ITL del telefono non è elencato né il server TFTP primario né il server TFTP di backup, è necessario sbloccare uno dei file prima che sia possibile salvare le modifiche all'opzione Server TFTP 2. In questo caso, il telefono elimina uno dei file quando vengono salvate le modifiche all'opzione Server TFTP 2. Un nuovo file CTL o ITL viene scaricato dal nuovo indirizzo del server TFTP 2. Se si dimentica di sbloccare il file CTL o ITL, è possibile modificare l'indirizzo del server TFTP 2 in uno dei file e cancellarlo premendo Cancella nel menu Configurazione protezione. Un nuovo file CTL o ITL viene scaricato dal nuovo indirizzo del server TFTP 2. Durante la ricerca del server TFTP, il telefono assegna la precedenza ai server TFTP assegnati manualmente a prescindere dal protocollo. Se nella configurazione sono inclusi i server TFTP IPv6 e IPv4, il telefono segue la priorità in base all'ordine di ricerca del server TFTP assegnando la priorità ai server TFTP IPv6 e ai server TFTP IPv4 assegnati manualmente. Il telefono cerca il server TFTP nell'ordine seguente: **1.** Server TFTP IPv4 assegnati manualmente **2.** Server IPv6 assegnati manualmente **3.** Server TFTP assegnati tramite DHCP **4.** Server TFTP assegnati tramite DHCPv6 **Nota** Per informazioni sui file CTL o ITL, consultare la Guida alla protezione di Cisco Unified Communications Manager.
Server BOOTP	Indica se il telefono ha ricevuto l'indirizzo IP da un server BOOTP invece che da un server DHCP.
Indirizzo DHCP rilasciato	Rilascia l'indirizzo IP assegnato tramite DHCP. È possibile modificare questo campo se il protocollo DHCP è abilitato. Se si desidera rimuovere il telefono dalla VLAN e liberare l'indirizzo IP per riassegnarlo, impostare questa opzione su Sì e premere Applica.

Campi di IPv6

Prima che sia possibile configurare le opzioni dell'impostazione IPv6 sul dispositivo, è necessario abilitare e configurare l'indirizzo IPv6 in Cisco Unified Communication Administration. I campi di configurazione del dispositivo seguenti si applicano alla configurazione IPv6:

- Modalità indirizzi IP
- Preferenza Modalità indirizzi IP per Segnalazione

Se IPv6 è abilitato nel cluster Unified, l'impostazione predefinita per la modalità indirizzi IP è IPv4 e IPv6. In questa modalità, il telefono acquisisce e utilizza un indirizzo IPv4 e un indirizzo IPv6. Può utilizzare l'indirizzo IPv4 e l'indirizzo IPv6 in base a come richiesto per il supporto. Il telefono utilizza l'indirizzo IPv4 o l'indirizzo IPv6 per la segnalazione del controllo chiamate.

Per ulteriori informazioni sulla distribuzione di IPv6, vedere la Guida alla distribuzione di IPv6 per Cisco Collaboration Systems versione 12.0.

È possibile impostare l'indirizzo IPv6 da uno dei menu seguenti:

- Se il Wi-Fi è disabilitato: **Impostazione Ethernet** > **Impostazione IPv6**
- Se il Wi-Fi è abilitato: **Impostazione client Wi-Fi** > **Impostazione IPv6**

Utilizzare la tastiera del telefono per immettere o modificare un indirizzo IPv6. Per immettere i due punti (:), premere l'asterisco (*) sulla tastiera. Per immettere le cifre esadecimali a, b e c, premere 2 sulla tastiera, scorrere per selezionare la cifra desiderata e premere **Invio**. Per immettere le cifre esadecimali d, e e f, premere 3 sulla tastiera, scorrere per selezionare la cifra desiderata e premere **Invio**.

Nella tabella seguente vengono descritte le informazioni correlate che è possibile trovare nel menu IPv6.

Tabella 22: Opzioni del menu Impostazione IPv6

Voce	Valore predefinito	Descrizione
DHCPv6 abilitato	Sì	Indica il metodo utilizzato dal telefono Se DHCPv6 è abilitato, il telefono ottier dell'RA inviata dal router abilitato per con stato (dal server DHCPv6) o senza
Indirizzo IPv6	::	Visualizza l'indirizzo solo IPv6 corrent La lunghezza di un indirizzo IPv6 valid • Otto set di cifre esadecimali separ • Formato compresso per comprime rappresentato da un doppio segno Se l'indirizzo IP viene assegnato tramit dell'indirizzo IPv6 e il router predefinit
Lunghezza prefisso IPv6	0	Visualizza la lunghezza del prefisso co prefisso. La lunghezza del prefisso della subnet
Router predefinito IPv6	::	Visualizza il router predefinito utilizzat predefinito.
Server DNS IPv6 1	::	Visualizza il server DNSv6 primario ut
Server DNS IPv6 2	::	Visualizza il server DNSv6 secondario secondario.
TFTP alternativo IPv6	No	Consente all'utente di abilitare l'uso di
Server TFTP IPv6 1	::	Visualizza il server TFTP IPv6 primari primario.
Server TFTP IPv6 2	::	(Facoltativo) Visualizza il server TFTP consente all'utente di impostare un nuo

Voce	Valore predefinito	Descrizione
Indirizzo IPv6 rilasciato	No	Consente all'utente di rilasciare le i

Impostazione del telefono per l'uso del server DHCP

Per abilitare il protocollo DHCP e consentire al server DHCP di assegnare automaticamente un indirizzo IP al telefono IP Cisco e indirizzare il telefono a un server TFTP, attenersi alla procedura seguente:

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione Ethernet** > **Impostazione IPv4**.

Passaggio 3 Per abilitare DHCP, impostare l'opzione DHCP abilitato su **Sì**. DHCP è abilitato per impostazione predefinita.

Passaggio 4 Per utilizzare un server TFTP alternativo, impostare l'opzione Server TFTP alternativo su **Sì** e immettere l'indirizzo IP del server TFTP.

Nota Rivolgersi all'amministratore di rete per stabilire se è necessario assegnare un server TFTP alternativo invece di utilizzare il server TFTP assegnato da DHCP.

Passaggio 5 Premere **Applica**.

Impostazione del telefono sull'utilizzo di un server diverso da DHCP

Se DHCP non è in uso, è necessario configurare in locale sul telefono l'indirizzo IP, la subnet mask, il server TFTP e il router predefinito.

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione Ethernet** > **Impostazione IPv4**.

Passaggio 3 Per disabilitare DHCP e impostare manualmente un indirizzo IP:

a) Impostare l'opzione DHCP abilitato su **No**.
b) Immettere l'indirizzo IP statico del telefono.
c) Immettere la subnet mask.
d) Immettere gli indirizzi IP del router predefinito.
e) Impostare l'opzione Server TFTP alternativo su **Sì** e immettere l'indirizzo IP del server TFTP 1.

Passaggio 4 Premere **Applica**.

Server di caricamento

Il server di caricamento viene utilizzato per ottimizzare il tempo di installazione per gli aggiornamenti del firmware del telefono e per scaricare la WAN mediante la memorizzazione delle immagini in locale, eliminando la necessità di attraversare il collegamento WAN per l'aggiornamento di ogni telefono.

È possibile impostare il server di caricamento su un indirizzo IP o nome del server TFTP diverso (diverso da Server TFTP 1 o Server TFTP 2) da cui è possibile recuperare il firmware del telefono per gli aggiornamenti. Quando l'opzione del server di caricamento è impostata, il telefono contatta il server designato per l'aggiornamento del firmware.

Nota L'opzione del server di caricamento consente di specificare un server TFTP alternativo soltanto per gli aggiornamenti del telefono. Il telefono continua a utilizzare il Server TFTP 1 o il Server TFTP 2 per ottenere i file di configurazione. L'opzione del server di caricamento non fornisce funzionalità di gestione dei processi e dei file, come ad esempio il trasferimento, la compressione o l'eliminazione dei file.

Il server di caricamento viene configurato dalla finestra Configurazione telefono aziendale. Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono** > **Configurazione telefono aziendale**.

Verifica dell'avvio del telefono

In seguito alla connessione del telefono IP Cisco a una fonte di alimentazione, viene avviato il processo diagnostico di avvio sul telefono in base ai passaggi seguenti.

1. Durante le varie fasi di avvio e la verifica dell'hardware da parte del telefono, i tasti funzione e sessione lampeggiano prima in giallo e poi in verde.
2. Nella schermata principale viene visualizzato il messaggio `Registrazione su Cisco Unified Communications Manager in corso`.

Se il telefono completa correttamente questi passaggi, il processo di avvio è andato a buon fine e il pulsante **Seleziona** rimane illuminato finché non viene selezionato.

Configurazione dei servizi telefonici per gli utenti

È possibile fornire agli utenti accesso ai servizi del telefono IP Cisco sul telefono IP. È inoltre possibile assegnare un tasto a diversi servizi del telefono. Questi servizi comprendono delle applicazioni XML e dei Java MIDlet firmati da Cisco che consentono di visualizzare i contenuti interattivi con testo e immagini sul telefono. Il telefono IP gestisce ogni servizio come applicazione separata. Tra gli esempi di tali servizi sono inclusi gli orari dei cinema della zona, le quotazioni azionarie e le previsioni del tempo.

Prima che un utente possa accedere a un servizio:

- Utilizzare Cisco Unified Communications Manager Administration per configurare i servizi non presenti per impostazione predefinita.
- L'utente deve abbonarsi ai servizi tramite Portale Cisco Unified Communications Self Care. Questa applicazione basata sul Web fornisce un'interfaccia utente grafica (GUI) per una configurazione limitata

dell'utente finale delle applicazioni del telefono IP. Tuttavia, un utente non può abbonarsi ad alcun servizio configurato come abbonamento aziendale.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Prima di configurare i servizi, raccogliere gli URL dei siti da impostare e verificare che gli utenti possano accedere a tali siti dalla rete di telefonia IP aziendale. Questa attività non è applicabile per i servizi predefiniti forniti da Cisco.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, scegliere **Dispositivo** > **Impostazioni dispositivo** > **Servizi telefonici**.

Passaggio 2 Verificare che gli utenti possano accedere a Portale Cisco Unified Communications Self Care, da dove possono selezionare e abbonarsi ai servizi configurati.

Consultare Gestione del portale Self Care, a pagina 83 per un riepilogo delle informazioni che occorre fornire agli utenti finali.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Modifica del modello del telefono di un utente

L'utente può modificare il modello del telefono di un utente. È possibile richiedere la modifica per una serie di motivi, ad esempio:

- È stato eseguito l'aggiornamento di Cisco Unified Communications Manager (Unified CM) a una versione del software che non supporta il modello di telefono.
- L'utente desidera un modello del telefono diverso dal modello corrente.
- Il telefono deve essere riparato o sostituito.

Unified CM identifica il telefono precedente e utilizza l'indirizzo MAC del telefono precedente per identificare la configurazione del vecchio telefono. Unified CM copia la configurazione del telefono precedente nella voce relativa al nuovo telefono. Il nuovo telefono ha la stessa configurazione del telefono precedente.

Se si sostituisce un telefono precedente con firmware SCCP con un modello del Telefono IP Cisco serie 8800, il nuovo telefono viene configurato per la modalità linea sessione.

Se il telefono precedente dispone di un modello di espansione tasti configurato, Unified CM copia contemporaneamente le informazioni relative al modulo di espansione sul nuovo telefono. Quando l'utente connette un modulo di espansione tasti compatibile al nuovo telefono, il nuovo modulo di espansione riceve le informazioni relative al modulo di espansione di cui è stata eseguita la migrazione.

Se il telefono precedente dispone di un modello di espansione tasti configurato e il nuovo telefono non supporta un modulo di espansione, Unified CM non copia le informazioni relative al modulo di espansione.

Limitazione: se il telefono precedente dispone di più linee o pulsanti di linea rispetto al nuovo telefono, il nuovo telefono non dispone delle linee o dei pulsanti di linea aggiuntivi configurati.

Il telefono viene riavviato al termine della configurazione.

Prima di iniziare

Impostare Cisco Unified Communications Manager in base alle istruzioni presenti nella *Guida alla configurazione delle funzionalità di Cisco Unified Communications Manager*.

È necessario un nuovo telefono non utilizzato e preinstallato con la versione del firmware 12.8(1) o successiva.

Procedura

Passaggio 1 Spegnere il telefono precedente.

Passaggio 2 Accendere il nuovo telefono.

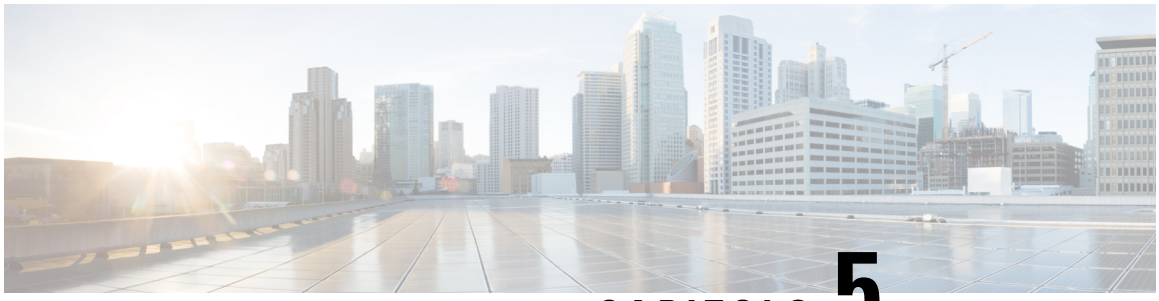
Passaggio 3 Sul nuovo telefono, selezionare **Sostituisci un telefono esistente**.

Passaggio 4 Immettere l'interno principale del telefono precedente.

Passaggio 5 Se al telefono precedente è stato assegnato un PIN, immettere il PIN.

Passaggio 6 Premere **Invia**.

Passaggio 7 Se è presente più di un dispositivo per l'utente, selezionare il dispositivo da sostituire e premere **Continua**.



CAPITOLO 5

Configurazione del telefono su Cisco Unified Communications Manager

Impostazione del telefono IP Cisco

Se la registrazione automatica non è abilitata e il telefono non è presente nel database di Cisco Unified Communications Manager, occorre configurare manualmente il telefono IP Cisco in Cisco Unified Communications Manager. Alcune attività in questa procedura sono facoltative, in base alle esigenze di utente e sistema.

Per ulteriori informazioni su Cisco Unified Communications Manager Administration, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Eseguire i passaggi della configurazione nella procedura seguente tramite Cisco Unified Communications Manager Administration.

Procedura

Passaggio 1 Raccogliere le seguenti informazioni sul telefono:

- Modello del telefono
- Indirizzo MAC
- Ubicazione fisica del telefono
- Nome o ID utente dell'utente del telefono

- Gruppo dispositivi
- Partizione, area ricerca chiamate e informazioni sulla posizione
- Numero di linee e numeri di rubrica (DN) associati da assegnare al telefono
- Utente Cisco Unified Communications Manager da associare al telefono
- Informazioni sull'uso del telefono con effetti sul modello dei pulsanti del telefono, sulle funzioni del telefono, sui servizi del telefono IP o sulle applicazioni del telefono

Tali informazioni forniscono un elenco dei requisiti di configurazione per l'impostazione dei telefoni e identificano le attività di configurazione preliminari da eseguire prima di configurare i singoli telefoni, come ad esempio l'impostazione dei modelli dei pulsanti del telefono.

Passaggio 2 Verificare di aver un numero sufficiente di licenze per il telefono.

Passaggio 3 Personalizzare i modelli dei pulsanti del telefono (se necessario) modificando il numero dei pulsanti di linea, dei pulsanti di chiamata rapida o dell'URL del servizio. Selezionare **Dispositivo** > **Impostazioni dispositivo** > **Modello pulsanti telefono** per creare e aggiornare i modelli.

In base alle esigenze degli utenti, è possibile aggiungere un pulsante Privacy, Tutte le chiamate o Mobilità interni telefonici.

Per ulteriori informazioni, consultare Modelli dei pulsanti del telefono, a pagina 200.

Passaggio 4 Definire i gruppi di dispositivi. Selezionare **Sistema** > **Gruppo dispositivi**.

I gruppi di dispositivi definiscono le caratteristiche comuni dei dispositivi, come regione, gruppo data/ora, modello softkey e informazioni MLPP.

Passaggio 5 Definire il profilo telefono comune. Selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**.

I profili del telefono comuni forniscono i dati richiesti dal server TFTP Cisco, oltre alle impostazioni comuni del telefono, come la funzione Non disturbare e le opzioni di controllo delle funzioni.

Passaggio 6 Definire un'area ricerca chiamate. In Cisco Unified Communications Manager Administration, fare clic su **Indirizzamento chiamata** > **Classe di controllo** > **Area ricerca chiamate**.

Un'area ricerca chiamate è un insieme di partizioni in cui avviene la ricerca per determinare le modalità di indirizzamento di un numero chiamato. L'area ricerca chiamate del dispositivo e l'area ricerca chiamate del numero di rubrica vengono utilizzate insieme. Il CSS del numero di rubrica ha la precedenza sul CSS del dispositivo.

Passaggio 7 Configurare un profilo di protezione per il protocollo e il tipo di dispositivo. Selezionare **Sistema** > **Protezione** > **Profilo di protezione telefono**.

Passaggio 8 Aggiungere e configurare il telefono compilando i campi richiesti nella finestra Configurazione telefono. L'asterisco (*) accanto al nome del campo indica un campo obbligatorio; ad esempio i campi Indirizzo MAC e Gruppo dispositivi.

Questo passaggio consente di aggiungere il dispositivo con le impostazioni predefinite al database di Cisco Unified Communications Manager.

Per informazioni sui campi di configurazione specifici del prodotto, consultare la sezione «?» Guida pulsanti nella finestra Configurazione telefono.

Nota Se si desidera aggiungere contemporaneamente telefono e utente al database Cisco Unified Communications Manager, consultare la documentazione della particolare versione di Cisco Unified Communications Manager.

Passaggio 9 Aggiungere e configurare i numeri di rubrica (linee) sul telefono compilando i campi richiesti nella finestra Configurazione numero di rubrica. L'asterisco (*) accanto al nome del campo indica un campo obbligatorio; ad esempio, Nr. di rubrica e Gruppo presenze.

Tramite questo passaggio è possibile aggiungere sul telefono dei numeri di rubrica primari e secondari e le funzioni associate.

Nota Se il numero di rubrica primario non viene configurato, l'utente visualizza il messaggio `Provisioning non effettuato` sul telefono.

Passaggio 10 Configurare i tasti di chiamata rapida e assegnare numeri di chiamata rapida.

Gli utenti possono modificare le impostazioni di chiamata rapida sui telefoni tramite il portale Self Care di Cisco Unified Communications.

Passaggio 11 Configurare i servizi del telefono IP Cisco Unified e assegnarli (facoltativo) per mettere a disposizione degli utenti i servizi del telefono IP.

Gli utenti possono aggiungere o modificare i servizi sui telefoni tramite il portale Self Care di Cisco Unified Communications.

Nota Gli utenti possono inoltre iscriversi al servizio del telefono IP soltanto se la casella di controllo Iscrizione aziendale è deselezionata quando il servizio del telefono IP viene configurato per la prima volta in Cisco Unified Communications Manager Administration.

Nota Alcuni servizi predefiniti forniti da Cisco vengono classificati tra le iscrizioni aziendali, pertanto l'utente non può aggiungerli tramite il portale Self Care. Tali servizi sono disponibili sul telefono per impostazione predefinita e possono essere rimossi soltanto disabilitandoli in Cisco Unified Communications Manager Administration.

Passaggio 12 Assegnare i servizi ai pulsanti programmabili (facoltativo) per fornire accesso a un servizio o a un URL del telefono IP.

Passaggio 13 Aggiungere le informazioni sugli utenti configurando i campi richiesti. L'asterisco (*) accanto al nome del campo indica un campo obbligatorio; ad esempio, i campi ID utente e Cognome. Questo passaggio consente di aggiungere le informazioni sull'utente alla rubrica globale di Cisco Unified Communications Manager.

Nota Assegnare una password (per il portale Self Care) e un PIN (per Mobilità interni telefonici Cisco ed Elenco personale).

Nota Se l'azienda utilizza una rubrica LDAP (Lightweight Directory Access Protocol) per memorizzare le informazioni sugli utenti, è possibile installare e configurare Cisco Unified Communications sull'uso della rubrica LDAP esistente.

Nota Se si desidera aggiungere contemporaneamente telefono e utente al database Cisco Unified Communications Manager, consultare la documentazione della particolare versione di Cisco Unified Communications Manager.

Passaggio 14 Associare un utente a un gruppo di utenti. Questo passaggio consente di assegnare gli utenti a un elenco comune di ruoli e autorizzazioni validi per tutti gli utenti di un gruppo. Gli amministratori possono gestire i

gruppi di utenti e le autorizzazioni per controllare il livello di accesso (e, quindi, il livello di sicurezza) degli utenti del sistema. Ad esempio, è necessario aggiungere gli utenti al gruppo di utenti finali Cisco CCM standard per consentire agli utenti di accedere al portale Self Care di Cisco Unified Communications Manager.

Passaggio 15 Associare l'utente a un telefono (facoltativo). Questo passaggio consente agli utenti di controllare il proprio telefono, come ad esempio la deviazione delle chiamate o l'aggiunta di servizi o di numeri di chiamata rapida.

Ad alcuni telefoni, come quelli nelle sale conferenze, non sono associati utenti.

Passaggio 16 Se non si è ancora nella finestra Configurazione utente finale, selezionare **Gestione utente** > **Utente finale** per effettuare alcune attività di configurazione finale. Tramite i campi Cerca e **Trova**, individuare l'utente (ad esempio John Doe), quindi fare clic sull'ID utente per andare alla finestra Configurazione utente finale relativa all'utente.

Passaggio 17 Nell'area Associazioni numero di rubrica della schermata, impostare l'interno principale dall'elenco a discesa.

Passaggio 18 Nell'area Informazioni mobilità, selezionare la casella Abilita mobilità.

Passaggio 19 Nell'area Informazioni autorizzazioni, utilizzare i pulsanti Gruppo utenti per aggiungere questo utente a uno dei gruppi di utenti.

Ad esempio, aggiungere l'utente a un gruppo definito come Gruppo utenti finali CCM standard.

Passaggio 20 Per visualizzare tutti i gruppi utenti configurati, selezionare **Gestione utente** > **Gruppo utenti**.

Passaggio 21 Nell'area Mobilità interni telefonici, selezionare la casella Abilita Mobilità interni telefonici nel cluster se l'utente può utilizzare tale servizio.

Passaggio 22 Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Individuazione dell'indirizzo MAC del telefono

Per aggiungere telefoni a Cisco Unified Communications Manager, è necessario individuare l'indirizzo MAC di un telefono.

Procedura

Effettuare una delle seguenti operazioni:

- Sul telefono, premere **Applicazioni**, selezionare **Informazioni telefono** e individuare il campo dell'indirizzo MAC.
- Osservare l'etichetta MAC sul retro del telefono.
- Aprire la pagina Web del telefono e fare clic su **Device Information**.

Metodi di aggiunta del telefono

Una volta installato il telefono IP Cisco, è possibile selezionare una delle opzioni seguenti per aggiungere i telefoni al database di Cisco Unified Communications Manager.

- Aggiunta di singoli telefoni con Cisco Unified Communications Manager Administration
- Aggiunta di più telefoni con lo strumento Bulk Administration Tool (BAT)
- Registrazione automatica
- Strumento BAT e TAPS (Tool for Auto-Registered Phones Support)

Per aggiungere i telefoni singolarmente o con lo strumento BAT, è necessario conoscere l'indirizzo MAC del telefono. Per ulteriori informazioni, consultare Individuazione dell'indirizzo MAC del telefono, a pagina 72.

Per ulteriori informazioni sullo strumento Bulk Administration Tool, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Aggiunta di singoli telefoni

Raccogliere l'indirizzo MAC e le informazioni sul telefono che si desidera aggiungere a Cisco Unified Communications Manager.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Passaggio 3 Selezionare il tipo di telefono.

Passaggio 4 Selezionare **Avanti**.

Passaggio 5 Completare le informazioni sul telefono, incluso l'indirizzo MAC.

Per istruzioni complete e informazioni su Cisco Unified Communications Manager, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Passaggio 6 Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Aggiunta di telefoni con modello telefono BAT

Lo strumento BAT (Bulk Administration Tool) di Cisco Unified Communications consente di effettuare delle operazioni in batch, inclusa la registrazione di più telefoni.

Per aggiungere i telefoni esclusivamente tramite lo strumento BAT (e non insieme allo strumento TAPS), è necessario ottenere l'indirizzo MAC corretto di ciascun telefono.

Per ulteriori informazioni sull'uso dello strumento BAT, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Da Cisco Unified Communications Administration, selezionare **Amministrazione globale** > **Telefoni** > **Modello telefono**.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Passaggio 3 Selezionare un tipo di telefono e fare clic su **Avanti**.

Passaggio 4 Immettere i dettagli relativi ai parametri specifici del telefono, come ad esempio quelli relativi al gruppo di dispositivi, al modello pulsanti del telefono e al profilo di protezione del dispositivo.

Passaggio 5 Fare clic su **Salva**.

Passaggio 6 Selezionare **Dispositivo** > **Telefono** > **Aggiungi nuovo** per aggiungere un telefono mediante il modello telefono BAT.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Aggiunta degli utenti a Cisco Unified Communications Manager

È possibile visualizzare e gestire le informazioni sugli utenti registrati in Cisco Unified Communications Manager. Cisco Unified Communications Manager consente inoltre agli utenti di eseguire le seguenti attività:

- Accedere alla rubrica aziendale e ad altre rubriche personalizzate da un telefono IP Cisco.
- Creare un Elenco personale.
- Impostare i numeri di chiamata rapida e di inoltro delle chiamate.
- Iscriversi ai servizi accessibili da un telefono IP Cisco.

Procedura

Passaggio 1 Per aggiungere gli utenti individualmente, consultare Aggiunta di un utente direttamente a Cisco Unified Communications Manager, a pagina 75.

Passaggio 2 Per aggiungere gli utenti in gruppi, utilizzare lo strumento Bulk Administration Tool. Tramite questo metodo è inoltre possibile impostare una password predefinita uguale per tutti gli utenti.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Aggiunta di un utente da una rubrica LDAP esterna

Se un utente è stato aggiunto a una rubrica LDAP (una rubrica diversa da quella del server Cisco Unified Communications), è possibile sincronizzare immediatamente tale rubrica LDAP sul server Cisco Unified Communications Manager su cui si sta aggiungendo l'utente e il relativo telefono.

Nota Se non si effettua immediatamente la sincronizzazione della rubrica LDAP sul server Cisco Unified Communications Manager, la successiva sincronizzazione automatica verrà pianificata in base alla pianificazione impostata per la sincronizzazione della rubrica LDAP nella finestra corrispondente. Prima che sia possibile associare un nuovo utente a un dispositivo, è necessario effettuare la sincronizzazione.

Procedura

Passaggio 1 Accedere a Cisco Unified Communications Manager Administration.

Passaggio 2 Selezionare **Sistema** > **LDAP** > **Rubrica LDAP**.

Passaggio 3 Utilizzare l'opzione **Trova** per individuare la rubrica LDAP.

Passaggio 4 Fare clic sul nome della rubrica LDAP.

Passaggio 5 Fare clic su **Esegui sincronizzazione completa adesso**.

Aggiunta di un utente direttamente a Cisco Unified Communications Manager

Se non si sta utilizzando una rubrica Lightweight Directory Access Protocol (LDAP), è possibile aggiungere direttamente un utente con Cisco Unified Communications Manager Administration attenendosi alla procedura seguente.

Nota Se LDAP è sincronizzato, non è possibile aggiungere un utente con Cisco Unified Communications Manager Administration.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Gestione utente** > **Utente finale**.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Passaggio 3 Nel riquadro Informazioni utente, immettere quanto segue:

- ID utente: immettere il nome di identificazione dell'utente finale. Dopo averlo creato, non è possibile modificare l'ID utente in Cisco Unified Communications Manager. È possibile utilizzare i seguenti caratteri speciali: =, +, <, >, #,;, \,, «» e gli spazi. **Esempio**: johndoe
- Password e Conferma password: immettere almeno cinque caratteri alfanumerici o speciali per la password dell'utente finale. È possibile utilizzare i seguenti caratteri speciali: =, +, <, >, #, ;, \, , «» e gli spazi.

- Cognome: immettere il cognome dell'utente finale. È possibile utilizzare i seguenti caratteri speciali: =, +,, #, ;, \, <, >, «» e gli spazi. **Esempio**: doe
- Numero di telefono: immettere il numero di rubrica principale dell'utente finale. Sui telefoni degli utenti finali possono essere presenti più linee. **Esempio**: 26640 (numero di telefono aziendale interno di John Doe)

Passaggio 4 Fare clic su **Salva**.

Aggiunta di un utente a un gruppo di utenti finali

Per aggiungere un utente al gruppo degli utenti finali standard di Cisco Unified Communications Manager, attenersi alla procedura seguente:

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Gestione utente** > **Impostazioni utente** > **Accedi al gruppo di controllo**.

Viene visualizzata la finestra Cerca ed elenca utenti.

Passaggio 2 Immettere i criteri di ricerca appropriati e fare clic su **Trova**.

Passaggio 3 Selezionare il collegamento **Utenti finali standard di CCM**. Viene visualizzata la finestra Configurazione gruppo di utenti relativa agli utenti finali standard di CCM.

Passaggio 4 Selezionare **Aggiungi utenti finali al gruppo**. Viene visualizzata la finestra Cerca ed elenca utenti.

Passaggio 5 Tramite le caselle di riepilogo a discesa Trova utente, individuare gli utenti da aggiungere e fare clic su **Trova**.

Viene visualizzato un elenco degli utenti corrispondenti ai criteri di ricerca.

Passaggio 6 Nell'elenco dei risultati, fare clic sulla casella di controllo accanto agli utenti da aggiungere al gruppo di utenti. Se l'elenco è lungo, utilizzare i collegamenti riportati in basso per visualizzare ulteriori risultati.

Nota Nell'elenco dei risultati della ricerca non vengono visualizzati gli utenti già appartenenti al gruppo.

Passaggio 7 Selezionare **Aggiungi selezionati**.

Associazione dei telefoni agli utenti

È possibile associare i telefoni agli utenti dalla finestra Utente finale Cisco Unified Communications Manager.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Gestione utente** > **Utente finale**.

Viene visualizzata la finestra Cerca ed elenca utenti.

Passaggio 2 Immettere i criteri di ricerca appropriati e fare clic su **Trova**.

Passaggio 3 Nell'elenco dei risultati, selezionare il collegamento corrispondente all'utente.

Passaggio 4 Selezionare **Associazione dispositivo**.

Viene visualizzata la finestra Associazione dispositivo utente.

Passaggio 5 Immettere i criteri di ricerca appropriati e fare clic su **Trova**.

Passaggio 6 Scegliere il dispositivo che si desidera associare all'utente selezionando la casella a sinistra del dispositivo.

Passaggio 7 Selezionare **Salva selezionati/modifiche** per associare il dispositivo all'utente.

Passaggio 8 Dall'elenco a discesa Collegamenti correlati nell'angolo in alto a destra della finestra, selezionare **Torna all'utente**, quindi fare clic su **Vai**.

Viene visualizzata la finestra Configurazione utente finale e i dispositivi associati selezionati vengono visualizzati nel riquadro Dispositivi controllati.

Passaggio 9 Selezionare **Salva selezionati/modifiche**.

SRST (Survivable Remote Site Telephony)

SRST (Survivable Remote Site Telephony) garantisce che le funzioni di base del telefono rimangano accessibili quando la connettività WAN viene interrotta. In questo scenario, il telefono può mantenere attiva una chiamata in corso e l'utente può accedere a un sottogruppo di funzioni disponibili. Quando si verifica il failover, l'utente riceve un messaggio di avviso sul telefono.

Per ulteriori informazioni sul firmware e il Survivable Remote Site Telephony supportati, consultare la pagina *Informazioni di compatibilità su Cisco Unified Survivable Remote Site Telephony* su Cisco.com (http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html).

Nella tabella seguente viene descritta la disponibilità delle funzioni durante il failover.

Tabella 23: Supporto funzione SRST

Funzione	Supportata	Note
Nuova chiamata	Sì	
Termina	Sì	
Ripeti	Sì	
Rispondi	Sì	
Attesa	Sì	
Riprendi	Sì	
Conferenza	Sì	
Conferenza a chiamate attive (Collega)	No	La softkey Ch. attive non viene visualizzata.

Funzione	Supportata	Note
Elenco partecipanti conferenza	No	
Trasferisci	Sì	
Trasferimento a chiamate attive (Trasferimento diretto)	No	
Risposta automatica	Sì	
Avviso di chiamata	Sì	
ID chiamante	Sì	
Indicatore acustico messaggio in attesa	Sì	
Pulsante linea programmabile Tutte le chiamate	Sì	
Pulsante linea programmabile Risposta	Sì	
Presentazione sessione unificata	Sì	Conferenza è la sola funzione supportata a causa di altre limitazioni delle funzioni.
Casella vocale	Sì	La casella vocale non verrà sincronizzata con altri utenti nel cluster Cisco Unified Communications Manager.
Inoltro di tutte le chiamate	Sì	Lo stato di deviazione è disponibile solo sul telefono su cui viene impostata la deviazione, in quanto non vi sono SLA (Shared Line Appearance) in modalità SRST. Le impostazioni di deviazione di tutte le chiamate non sono mantenute durante il failover in SRST da Cisco Unified Communications Manager, oppure dal failback SRST a Communications Manager. Eventuali deviazioni di tutte le chiamate originali attive in Communications Manager devono essere indicate quando il dispositivo si ricollega a Communications Manager dopo il failover.
Chiamata rapida	Sì	
Pulsante linea programmabile IRL servizio	Sì	
A casella vocale (ImmDev)	No	La softkey ImmDev non viene visualizzata.

Funzione	Supportata	Note
Filtri linea	Parziale	Le linee sono supportate ma non possono essere condivise.
Monitoraggio parcheggio	No	La softkey ParChi non viene visualizzata.
Includi	No	La softkey Inclus. non viene visualizzata.
Indicazione avanzata messaggio in attesa	No	Sullo schermo del telefono non vengono visualizzati i simboli del numero di messaggi. Viene visualizzata solo l'icona di messaggio in attesa.
Parcheggio chiamate indirizzate	No	La softkey non viene visualizzata.
Indicatore di stato	Parziale	Il tasto funzione Indicatore di stato funziona come quelli di chiamata rapida.
Ripristino attesa	No	Le chiamate restano in attesa a tempo indefinito.
Attesa remota	No	Le chiamate vengono visualizzate come chiamate in attesa locali.
Conferenza automatica	No	La softkey ConfAut non viene visualizzata.
RispAss	No	La softkey non genera nessuna azione.
Risposta per assente di gruppo	No	La softkey non genera nessuna azione.
Risposta per altri gruppi	No	La softkey non genera nessuna azione.
ID chiamata indesiderata	No	La softkey non genera nessuna azione.
QRT	No	La softkey non genera nessuna azione.
Gruppo di ricerca	No	La softkey non genera nessuna azione.
Interfono	No	La softkey non genera nessuna azione.
Mobilità	No	La softkey non genera nessuna azione.
Privacy	No	La softkey non genera nessuna azione.
Prenotazione di chiamata	No	La softkey Prenota non viene visualizzata.
Video	Sì	La videoconferenza non è supportata.
Video	Sì	La videoconferenza non è supportata.
Linea condivisa	No	

Funzione	Supportata	Note
Chiamata rapida con indicatore di stato	Sì	

Enhanced Survivable Remote Site Telephony

E-SRST (Enhanced Survivable Remote Site Telephony) garantisce che le funzioni aggiuntive del telefono rimangano accessibili quando la connettività WAN viene interrotta. Oltre alle funzioni supportate da SRST (Survivable Remote Site Telephony), E-SRST supporta quanto segue:

- Linea condivisa
- Indicatore di stato
- Videochiamate

Per ulteriori informazioni sul firmware e il Survivable Remote Site Telephony supportati, consultare la pagina *Informazioni di compatibilità su Cisco Unified Survivable Remote Site Telephony* su Cisco.com (http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html).

Regole di composizione applicazione

Le regole di composizione applicazione vengono utilizzate per convertire i numeri dei contatti del cellulare condivisi in numeri componibili sulla rete. Le regole di composizione applicazione non si applicano se l'utente compone un numero manualmente o se il numero viene modificato prima che l'utente effettui la chiamata.

Le regole di composizione applicazione sono impostate in Cisco Unified Communications Manager.

Per ulteriori informazioni sulle regole di composizione, consultare *Guida alla configurazione di sistema per Cisco Unified Communications Manager*, capitolo «Configurazione delle regole di composizione».

Configurazione delle regole di composizione applicazione

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Indirizzamento chiamata** > **Regole di composizione** > **Regole di composizione applicazione**.

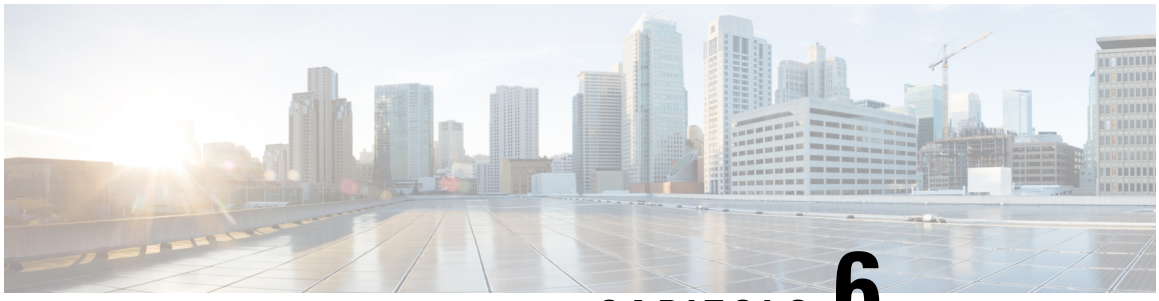
Passaggio 2 Selezionare **Aggiungi nuova** per creare una nuova regola di composizione applicazione oppure selezionare una regola di composizione applicazione esistente da modificare.

Passaggio 3 Completare i campi seguenti:

- **Nome** In questo campo è riportato il nome univoco della regola di composizione che può contenere fino a 20 caratteri alfanumerici e qualsiasi combinazione di spazi, punti (.), trattini (-) e caratteri di sottolineatura (_).
- **Descrizione** In questo campo è riportata una breve descrizione della regola di composizione.

- **Cifre iniziali numero**. In questo campo sono riportate le cifre iniziali dei numeri di rubrica ai quali si desidera applicare la regola di composizione applicazione.
- **Numero di cifre**. In questo campo obbligatorio sono riportate le cifre iniziali dei numeri di rubrica ai quali si desidera applicare la regola di composizione applicazione.
- **Totale cifre da rimuovere**. In questo campo obbligatorio è riportato il numero di cifre che Cisco Unified Communications Manager deve rimuovere dai numeri di rubrica per applicare la regola di composizione.
- **Prefisso con combinazione**. In questo campo obbligatorio è riportata la combinazione da anteporre ai numeri di rubrica per i quali viene applicata la regola di composizione applicazione.
- **Priorità regola di composizione applicazione**. In questo campo vengono visualizzate le informazioni immesse per l'opzione Prefisso con combinazione. Questo campo consente di impostare l'ordine di priorità delle regole di composizione applicazione.

Passaggio 4 Riavviare Cisco Unified Communications Manager.



CAPITOLO 6

Gestione del portale Self Care

Panoramica del portale Self Care

Dal portale Self Care di Cisco Unified Communications, gli utenti possono personalizzare e gestire le funzioni e le impostazioni del telefono.

In qualità di amministratore, è possibile controllare l'accesso al portale Self Care. È necessario inoltre fornire delle informazioni agli utenti per consentire loro di accedere al portale Self Care.

Prima che un utente possa accedere al portale Self Care di Cisco Unified Communications, è necessario utilizzare Cisco Unified Communications Manager Administration per aggiungere l'utente a un gruppo di utenti finali Cisco Unified Communications Manager standard.

È necessario comunicare agli utenti finali le informazioni seguenti sul portale Self Care:

- L'URL per accedere all'applicazione. L'URL è:

  `https://<server_name:portnumber>/ucmuser/`, dove server_name indica l'host su cui è installato il server Web e portnumber indica il numero di porta dell'host.

- Un ID utente e una password predefinita per accedere all'applicazione.

- Una panoramica delle attività che gli utenti possono effettuare sul portale.

Queste impostazioni corrispondono ai valori immessi quando si è aggiunto l'utente a Cisco Unified Communications Manager.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione dell'accesso degli utenti al portale Self Care

Per consentire agli utenti di accedere al portale Self Care, è necessario autorizzare l'accesso.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Gestione utenti** > **Utente finale**.
Passaggio 2	Cercare l'utente.
Passaggio 3	Fare clic sul collegamento ID utente.
Passaggio 4	Assicurarsi che per l'utente siano stati configurati un codice PIN e una password.
Passaggio 5	Nella sezione Informazioni sulle autorizzazioni, assicurarsi che l'elenco Gruppi includa gli **utenti finali standard di CCM**.
Passaggio 6	Selezionare **Salva**.

Personalizzazione della visualizzazione del portale Self Care

La maggior parte delle opzioni viene visualizzata nel portale Self Care. Tuttavia, è necessario impostare le opzioni seguenti mediante le impostazioni di configurazione dei parametri Enterprise in Cisco Unified Communications Manager Administration:

- Mostra impostazioni suoneria
- Mostra impostazioni etichetta linea

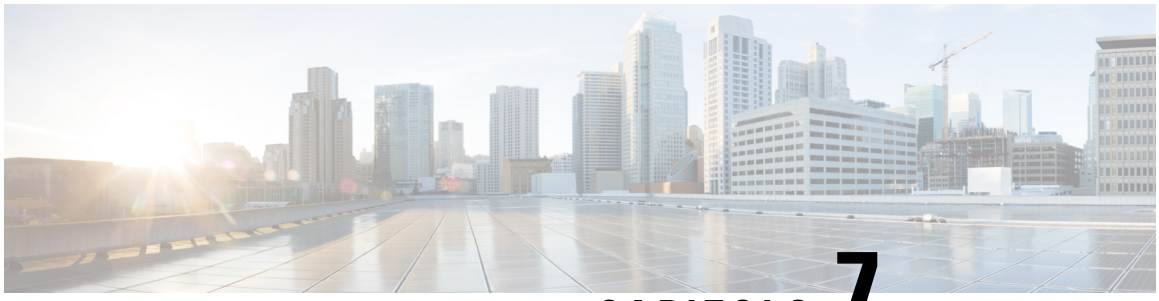
Nota Queste impostazioni si applicano a tutte le pagine del portale Self Care del proprio sito.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Sistema** > **Parametri aziendali**.
Passaggio 2	Nell'area del portale Self Care, impostare il campo **Server predefinito portale Self Care**.
Passaggio 3	Abilitare o disabilitare i parametri a cui gli utenti possono accedere nel portale.
Passaggio 4	Selezionare **Salva**.

PARTE III

Amministrazione del telefono IP Cisco



CAPITOLO 7

Protezione del telefono IP Cisco

Miglioramento della protezione della rete telefonica

È possibile consentire a Cisco Unified Communications Manager 11.5(1) e 12.0(1) di funzionare in un ambiente con protezione avanzata. Grazie a tali miglioramenti, la rete telefonica funziona rispettando una serie di severi controlli per la gestione della protezione e dei rischi al fine di proteggere i singoli utenti.

Cisco Unified Communications Manager 12.5 (1) non supporta un ambiente con protezione avanzata. È necessario disabilitare FIPS prima di eseguire l'aggiornamento a Cisco Unified Communications Manager 12.5 (1) altrimenti TFTP e altri servizi non funzionano correttamente.

L'ambiente con protezione avanzata include le seguenti funzionalità:

- Autenticazione per la ricerca di contatti.
- TCP come protocollo predefinito per la registrazione di controllo remota.
- Modalità FIPS.
- Criteri migliorati per le credenziali.
- Supporto della famiglia SHA-2 di hash per la firma digitale.
- Supporto per una dimensione di chiave RSA di 512 e 4096 bit.

Con Cisco Unified Communications Manager versione 14.0 e Firmware del telefono IP Cisco versione 14.0 e successive, i telefoni supportano l'autenticazione SIP OAuth.

OAuth è supportato per il protocollo Proxy TFTP (Trivial File Transfer Protocol) con Cisco Unified Communications Manager versione 14.0(1)SU1 o successiva e la versione del firmware del telefono IP Cisco 14.1(1). Proxy TFTP e OAuth perProxy TFTP non sono supportati su MRA (Mobile Remote Access).

Per ulteriori informazioni sulla protezione, vedere:

- *Guida alla configurazione del sistema di Cisco Unified Communications Manager* versione 14.0(1) o successive (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).

- *Panoramica sulla protezione del telefono IP Cisco serie 7800 e 8800* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)
- *Guida alla sicurezza di Cisco Unified Communications Manager* (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

Nota Il telefono IP Cisco può memorizzare solo un numero limitato di file ITL (Identity Trust List). I file ITL non possono superare il limite di 64 K sul telefono, quindi limitare il numero di file ITL che Cisco Unified Communications Manager invia al telefono.

Funzioni di protezione supportate

Le funzioni di protezione consentono di proteggere da molte minacce, comprese quelle all'identità del telefono e ai dati. Queste funzioni stabiliscono e mantengono flussi di comunicazioni autenticati tra il telefono e il server Cisco Unified Communications Manager e garantiscono che il telefono utilizzi solo file con firma digitale.

Cisco Unified Communications Manager Release 8.5(1) e versioni successive comprende Protezione per valore predefinito, che fornisce le seguenti funzioni di protezione ai telefoni IP Cisco senza dover eseguire il client CTL:

- Firma dei file di configurazione del telefono
- Crittografia del file di configurazione del telefono
- HTTPS con Tomcat e altri servizi Web

Nota Le funzioni dei supporti e di segnalazione protette richiedono ancora l'esecuzione del client CTL e l'utilizzo di eToken hardware.

Tramite l'implementazione della protezione nel sistema di Cisco Unified Communications Manager è possibile impedire il furto di identità del telefono e del server Cisco Unified Communications Manager, l'alterazione dei dati e della segnalazione delle chiamate e del flusso multimediale.

Per ridurre queste minacce, la rete di telefonia IP Cisco stabilisce e mantiene dei flussi di comunicazione protetti (crittografati) tra i telefoni e il server, aggiunge una firma digitale ai file prima del trasferimento sui telefoni e crittografa i flussi multimediali e la segnalazione delle chiamate tra i telefoni IP Cisco.

Dopo aver eseguito le attività necessarie associate a CAPF (Certificate Authority Proxy Function), sui telefoni viene installato un LSC (Locally Significant Certificate). È possibile utilizzare Cisco Unified Communications Manager Administration per configurare un LSC, come descritto nella Guida alla protezione di Cisco Unified Communications Manager. In alternativa, è possibile avviare l'installazione di un LSC dal menu Impostazione protezione del telefono. Questo menu consente inoltre di aggiornare o rimuovere un LSC.

Non è possibile utilizzare un LSC come certificato utente per EAP-TLS con l'autenticazione WLAN.

I telefoni utilizzano il profilo di protezione che ne definisce lo stato di protezione. Per informazioni sull'applicazione del profilo di protezione al telefono, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Se vengono configurate le impostazioni relative alla protezione in Cisco Unified Communications Manager Administration, il file di configurazione del telefono conterrà delle informazioni riservate. Per garantire la privacy del file di configurazione, è necessario configurarlo per la crittografia. Per informazioni dettagliate, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

I telefoni IP Cisco serie 8800 sono conformi agli Standard FIPS (Federal Information Processing Standard). Per il corretto funzionamento della modalità FIPS, è necessario impostare una dimensione di chiave di 2048 bit o superiore. Se la dimensione della chiave del certificato non è 2048 bit o superiore, il telefono non viene registrato con Cisco Unified Communications Manager e sul telefono viene visualizzato il messaggio `Impossibile registrare il telefono. La dimensione della chiave del certificato non è conforme a FIPS.`

Se il telefono ha un LSC, prima di abilitare FIPS, è necessario impostare la dimensione della chiave LSC su 2048 bit o su una dimensione superiore.

Nella tabella seguente viene presentata una panoramica delle funzioni di protezione supportate dai telefoni. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Per visualizzare le impostazioni di protezione correnti su un telefono, tra cui la modalità Protezione, Trust list e l'autenticazione 802.1X, premere **Applicazioni** e scegliere **Impostazioni amministratore** > **Impostazione protezione**.

Tabella 24: Panoramica delle funzioni di protezione

Funzione	Descrizione
Autenticazione immagine	I file binari con firma (con estensione .sbn) impediscono l'alterazione tramite l'immagine del firmware prima che tale immagine venga caricata sul telefono. La manomissione con l'immagine impedisce al telefono di eseguire il processo di autenticazione e determina il rifiuto della nuova immagine.
Crittografia immagine	I file binari crittografati (con estensione .sebn) impediscono l'alterazione tramite l'immagine del firmware prima che tale immagine venga caricata sul telefono. La manomissione con l'immagine impedisce al telefono di eseguire il processo di autenticazione e determina il rifiuto della nuova immagine.
Installazione del certificato del sito del cliente	Ogni telefono IP Cisco richiede un certificato univoco per l'autenticazione del dispositivo. Nei telefoni è incluso un certificato MIC (Manufacturing Installed Certificate), ma per ulteriore protezione, è possibile specificare l'installazione di un certificato su Cisco Unified Communications Manager Administration tramite CAPF (Certificate Authority Proxy Function). In alternativa, è possibile installare un LSC (Locally Significant Certificate) dal menu di configurazione della protezione del telefono.
Autenticazione dispositivo	Si verifica tra il server Cisco Unified Communications Manager e il telefono quando ciascuna entità accetta il certificato dell'altra. Determina se deve essere stabilita una connessione protetta tra il telefono e un server Cisco Unified Communications Manager e, se necessario, crea un percorso di segnalazione protetto tra le due entità mediante il protocollo TLS. Cisco Unified Communications Manager non registra i telefoni a meno che non sia in grado di autenticarli.

Funzione	Descrizione
Autenticazione file	Convalida i file con firma digitale scaricati dal telefono. Il telefono convalida le firme per garantire che i file non siano stati alterati dopo la creazione. I file che non vengono autenticati non vengono scritti nella memoria flash del telefono. Il telefono rifiuta tali file senza ulteriore elaborazione.
Crittografia file	La crittografia impedisce la divulgazione delle informazioni riservate durante il passaggio del file verso il telefono. Inoltre, il telefono convalida la firma per garantire che il file non sia stato alterato dopo la creazione. I file che non vengono autenticati non vengono scritti nella memoria flash del telefono. Il telefono rifiuta tali file senza ulteriore elaborazione.
Autenticazione segnalazione	Utilizza il protocollo TLS per confermare che i pacchetti di segnalazione non siano stati alterati durante la trasmissione.
MIC (Manufacturing Installed Certificate)	Ciascun telefono IP Cisco contiene un certificato MIC (manufacturing installed certificate) univoco, utilizzato per l'autenticazione del dispositivo. Il certificato MIC rappresenta una garanzia univoca e permanente di identità per il telefono e consente a Cisco Unified Communications Manager di autenticare il telefono.
Crittografia supporti	Utilizza il protocollo SRTP per garantire che i flussi multimediali tra i dispositivi supportati risultino protetti e che solo il dispositivo previsto riceva e legga i dati. Comprende la creazione di una coppia di chiavi primaria di supporti per i dispositivi, la consegna delle chiavi ai dispositivi e la protezione della consegna delle chiavi durante il loro trasporto.
CAPF (Certificate Authority Proxy Function)	Implementa parti della procedura di generazione del certificato che richiedono elevati sforzi di elaborazione da parte del telefono e interagisce con il telefono per la generazione di chiavi e l'installazione del certificato. È possibile configurare CAPF in modo che richieda certificati da autorità di certificazione specificate dal cliente per conto del telefono, oppure per generare certificati localmente.
Profilo di protezione	Definisce se il telefono è in stato non protetto, autenticato, crittografato o protetto. Le altre voci di questa tabella descrivono le funzioni di protezione.
File di configurazione crittografati	Consente di garantire la privacy dei file di configurazione del telefono.
Disabilitazione facoltativa del server Web per i telefoni	Per ragioni di protezione, è possibile impedire l'accesso alle pagine Web del telefono (in cui vengono visualizzate diverse statistiche di operatività del telefono) e del portale Self Care.
Aumento della sicurezza del telefono	Ulteriori opzioni di protezione, controllabili da Cisco Unified Communications Manager Administration: • Disabilitazione della porta PC • Disabilitazione di Gratuitous ARP (GARP) • Disabilitazione dell'accesso alla VLAN vocale del PC • Disabilitazione dell'accesso ai menu delle impostazioni o accesso limitato soltanto al menu delle preferenze e salvataggio esclusivamente delle modifiche al volume • Disabilitazione dell'accesso alle pagine Web di un telefono • Disabilitazione della porta dell'accessorio Bluetooth • Limitazione delle crittografie TLS

Funzione	Descrizione
Autenticazione 802.1X	Il telefono IP Cisco può utilizzare l'autenticazione 802.1X per richiedere e ottenere accesso alla rete. Per ulteriori informazioni, vedere Autenticazione 802.1X, a pagina 113.
Failover SIP protetto per SRST	In seguito alla configurazione di un riferimento SRST (Survivable Remote Site Telephony) per la protezione e alla reimpostazione dei dispositivi dipendenti in Cisco Unified Communications Manager Administration, il server TFTP aggiunge il certificato SRST al file cnf.xml del telefono e invia tale file al telefono. Un telefono protetto utilizza quindi una connessione TLS per interagire con il router SRST compatibile.
Crittografia segnalazione	Garantisce che tutti i messaggi di segnalazione SIP inviati tra il dispositivo e il server Cisco Unified Communications Manager siano crittografati.
Avviso aggiornamento Trust List	In caso di aggiornamenti della Trust List sul telefono, Cisco Unified Communications Manager riceve un avviso che indica il completamento o la mancata riuscita dell'aggiornamento. Per ulteriori informazioni, consultare la tabella seguente.

Crittografia AES 256	Quando sono collegati a Cisco Unified Communications Manager Release 10.5(2) e versioni successive, i telefoni supportano la crittografia AES 256 per TLS e SIP per la segnalazione e la crittografia dei supporti. Ciò consente ai telefoni di avviare e supportare le connessioni TLS 1.2 tramite codici basati su AES-256 conformi a standard SHA-2 (Secure Hash Algorithm) e compatibili con FIPS (Federal Information Processing Standards). Le crittografie includono:
	• Per connessioni TLS:
	  • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	  • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	• Per sRTP:
	  • AEAD_AES_256_GCM
	  • AEAD_AES_128_GCM
	Per ulteriori informazioni, consultare la documentazione di Cisco Unified Communications Manager.

Certificati Elliptic Curve Digital Signature Algorithm (ECDSA)	Come parte della certificazione dei criteri comuni (CC), Cisco Unified Communications Manager ha aggiunto i certificati ECDSA nella versione 11.0. Ciò ha effetto su tutti i prodotti VOS (Voice Operating System), dalla versione CUCM 11.5 e successive.

Nella tabella seguente vengono elencati i messaggi di avviso sull'aggiornamento della Trust List e il relativo significato. Per ulteriori informazioni, consultare la documentazione di Cisco Unified Communications Manager.

Tabella 25: Messaggi di avviso aggiornamento Trust List

Codice e messaggio	Descrizione
1 - TL_SUCCESS	Nuovo CTL e/o ITL ricevuto
2 - CTL_INITIAL_SUCCESS	Nuovo CTL ricevuto, nessuna TL esistente

Codice e messaggio	Descrizione
3 - ITL_INITIAL_SUCCESS	Nuovo ITL ricevuto, nessuna TL esistente
4 - TL_INITIAL_SUCCESS	Nuovi CTL e ITL ricevuti, nessuna TL esistente
5 - TL_FAILED_OLD_CTL	Aggiornamento alla nuova CTL non riuscito, ma TL precedente disponibile
6 - TL_FAILED_NO_TL	Aggiornamento alla nuova TL non riuscito e nessuna TL precedente presente
7 - TL_FAILED	Errore generico
8 - TL_FAILED_OLD_ITL	Aggiornamento alla nuova ITL non riuscito, ma TL precedente disponibile
9 - TL_FAILED_OLD_TL	Aggiornamento alla nuova TL non riuscito, ma TL precedente disponibile

Nel menu Impostazione protezione vengono fornite delle informazioni sulle diverse impostazioni di protezione. Il menu fornisce inoltre accesso al menu Trust List e indica se il file CTL o ITL è installato sul telefono.

Nella tabella seguente vengono descritte le opzioni disponibili nel menu Impostazione protezione.

Tabella 26: Menu Impostazione protezione

Opzione	Descrizione	Per modificare
Modalità Protezione	Visualizza la modalità di protezione impostata per il telefono.	Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**. L'impostazione viene visualizzata nell'area Informazioni specifiche protocollo della finestra Configurazione telefono.
LSC	Indica se sul telefono è installato (Sì) o meno (No) un certificato LCS, utilizzato per le funzioni di protezione.	Per informazioni sulla gestione del certificato LSC del telefono, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Opzione	Descrizione	Per modificare
Trust List	La Trust List fornisce dei menu secondari per i file di configurazione firmati, CTL e ITL. Nel menu secondario File CTL vengono visualizzati i contenuti del file CTL. Nel menu secondario File ITL vengono visualizzati i contenuti del file ITL. Nel menu Trust List vengono visualizzate anche le seguenti informazioni: • Firma CTL: l'hash SHA1 del file CTL • Server Unified CM/TFTP: il nome del server Cisco Unified Communications Manager e TFTP utilizzato dal telefono. Visualizza un'icona di certificato se sul server è presente un certificato installato. • Server CAPF: il nome del server CAPF utilizzato dal telefono. Visualizza un'icona di certificato se sul server è presente un certificato installato. • Router SRST: l'indirizzo IP del router SRST attendibile che può essere utilizzato dal telefono. Visualizza un'icona di certificato se sul server è presente un certificato installato.	Per ulteriori informazioni, consultare Impostazione di un LSC (Locally Significant Certificate), a pagina 93.
Autenticazione 802.1X	Consente di abilitare l'autenticazione 802.1X per il telefono in uso.	Consultare Autenticazione 802.1X, a pagina 113.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione di un LSC (Locally Significant Certificate)

Questa attività è valida per l'impostazione di un LSC con il metodo stringa di autenticazione.

Prima di iniziare

Assicurarsi che le configurazioni delle impostazioni di sicurezza appropriate di Cisco Unified Communications Manager e di Certificate Authority Proxy Function (CAPF) siano complete:

- Il file CTL o ITL dispone di un certificato CAPF.
- In Cisco Unified Communications Operating System Administration, verificare che il certificato CAPF sia installato.
- Il certificato CAPF è in esecuzione e configurato.

Per ulteriori informazioni su queste impostazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Ottenere il codice di autenticazione CAPF impostato al momento della configurazione di CAPF.

Passaggio 2 Sul telefono, premere **Applicazioni** .

Passaggio 3 Scegliere **Impostazioni amministratore** > **Impostazione protezione**.

Nota È possibile controllare l'accesso al menu delle impostazioni mediante il campo Accesso alle impostazioni nella finestra Configurazione telefono di Cisco Unified Communications Manager Administration.

Passaggio 4 Selezionare **LSC** e premere **Seleziona** oppure **Aggiorna**.

Il telefono richiede una stringa di autenticazione.

Passaggio 5 Immettere il codice di autenticazione e premere **Invia**.

A seconda della configurazione del certificato CAPF, il telefono avvia l'installazione, l'aggiornamento o la rimozione del certificato LSC. Durante la procedura, nel campo dell'opzione del certificato LSC nel menu Configurazione protezione vengono visualizzati dei messaggi tramite i quali è possibile monitorare l'avanzamento. Al termine della procedura, sul telefono viene visualizzato il messaggio Installato o Non installato.

Il completamento del processo di installazione, aggiornamento o rimozione del certificato LSC potrebbe richiedere diversi istanti.

Se la procedura di installazione del telefono riesce correttamente, viene visualizzato il messaggio `Installato`. Se sul telefono viene visualizzato il messaggio `Non installato`, la stringa di autorizzazione potrebbe essere errata o il telefono potrebbe non essere abilitato per l'aggiornamento. Se l'operazione CAPF elimina il certificato LSC, sul telefono viene visualizzato il messaggio `Non installato` per indicare che l'operazione è riuscita correttamente. Il server CAPF registra i messaggi di errore. Fare riferimento alla documentazione del server CAPF per consultare i registri e comprendere il significato dei messaggi di errore.

Abilitazione della modalità FIPS

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono** e individuare il telefono.

Passaggio 2 Accedere all'area Configurazione specifica del prodotto.

Passaggio 3 Impostare il parametro **Modalità FIPS** su Abilitato.

Passaggio 4 Selezionare **Applica configurazione**.

Passaggio 5 Selezionare **Salva**.

Passaggio 6 Riavviare il telefono.

Protezione delle chiamate

Se su un telefono sono state implementate delle funzioni di protezione, è possibile identificare le chiamate protette tramite le icone visualizzate sullo schermo del telefono. È inoltre possibile determinare se il telefono connesso è sicuro e protetto se all'inizio della chiamata viene riprodotta una tonalità di sicurezza.

In una chiamata protetta, tutti i flussi multimediali e di segnalazione delle chiamate sono crittografati. Le chiamate protette offrono un livello elevato di sicurezza e aggiungono integrità e privacy alla chiamata. Se una chiamata in corso è crittografata, la relativa icona sulla destra del timer di durata della chiamata nello schermo del telefono cambia nell'icona seguente:  .

Nota Se la chiamata viene indirizzata tramite fasi di chiamata non IP, ad esempio PSTN, la chiamata potrebbe non essere protetta anche se è crittografata all'interno della rete IP e dispone di un'icona a forma di lucchetto associata.

All'inizio di una chiamata protetta, viene riprodotta una tonalità di sicurezza per indicare che anche l'audio ricevuto e trasmesso sull'altro telefono connesso è protetto. Se la chiamata viene connessa a un telefono non protetto, la tonalità di sicurezza non viene riprodotta.

Nota Le chiamate protette sono supportate soltanto per le connessioni tra due telefoni. Alcune funzioni, come le chiamate in conferenza e le linee condivise, non sono disponibili se sono configurate le chiamate protette.

Quando un telefono è configurato come protetto (crittografato e attendibile) in Cisco Unified Communications Manager, è possibile assegnargli uno stato «protetto». Se lo si desidera, è possibile configurare la riproduzione di un tono indicativo all'inizio di una chiamata sul telefono protetto:

- Dispositivo protetto: per modificare lo stato di un telefono sicuro su protetto, selezionare la casella di controllo Dispositivo protetto nella finestra Configurazione telefono in Cisco Unified Communications Manager Administration (**Dispositivo** > **Telefono**).
- Riproduci tono indicativo protetto: per abilitare la riproduzione di un tono indicativo protetto o non protetto sul telefono protetto, impostare l'impostazione Riproduci tono indicativo protetto su Vero. Per impostazione predefinita, l'impostazione Riproduci tono indicativo protetto è impostata su Falso. Impostare questa opzione in Cisco Unified Communications Manager Administration (**Sistema** > **Parametri servizio**). Selezionare il server, quindi il servizio di Unified Communications Manager. Nella finestra Configurazione parametri servizio, selezionare l'opzione nell'area Funzione - Tonalità di sicurezza. L'impostazione predefinita è Falso.

Identificazione delle chiamate in conferenza protette

È possibile avviare una chiamata in conferenza protetta e monitorare il livello di protezione dei partecipanti. Le chiamate in conferenza protette vengono effettuate mediante la procedura seguente:

1. Un utente avvia la conferenza da un telefono protetto.
2. Cisco Unified Communications Manager assegna un ponte conferenza protetto alla chiamata.
3. Durante l'aggiunta dei partecipanti, Cisco Unified Communications Manager verifica la modalità di protezione di ciascun telefono e mantiene il livello di protezione per la conferenza.

4. Il livello di protezione della chiamata in conferenza viene visualizzato sul telefono. Per le conferenze protette viene visualizzata l'icona di protezione a destra di **Conferenza** sullo schermo del telefono.

Nota Le chiamate protette sono supportate per le connessioni tra due telefoni. Alcune funzioni, come ad esempio Chiamata in conferenza, Linee condivise e Mobilità interni telefonici, non sono disponibili sui telefoni protetti se sono configurate le chiamate protette.

Nella tabella seguente vengono fornite delle informazioni sulle modifiche dei livelli di protezione delle conferenze in base al livello di protezione del telefono da cui è stata avviata la chiamata in conferenza, ai livelli di protezione dei partecipanti e alla disponibilità dei ponti conferenza protetti.

Tabella 27: Limitazioni di protezione per le chiamate in conferenza

Livello di protezione del telefono dell'utente che ha avviato la conferenza	Funzione utilizzata	Livello di protezione dei partecipanti	Risultati dell'azione
Non protetto	Conferenza	Protetto	Ponte conferenza non protetto Conferenza non protetta
Protetto	Conferenza	Almeno un membro non è protetto.	Ponte conferenza protetto Conferenza non protetta
Protetto	Conferenza	Protetto	Ponte conferenza protetto Conferenza con livello di protezione crittogra
Non protetto	Conferenza automatica	Il livello minimo di protezione è crittografato.	L'utente che ha avviato la conferenza riceve il m `Non rispetta il livello di prote` `chiamata rifiutata`.
Protetto	Conferenza automatica	Il livello minimo di protezione non è protetto.	Ponte conferenza protetto Nella conferenza vengono accettate tutte le ch

Identificazione delle chiamate protette

È possibile effettuare una chiamata protetta se il telefono in uso e il telefono dell'altra parte sono configurati per le chiamate protette. L'altro telefono può trovarsi sulla stessa rete IP Cisco o su una rete al di fuori della rete IP. È possibile effettuare delle chiamate protette soltanto tra due telefoni. In seguito all'impostazione del ponte conferenza, per le chiamate in conferenza dovrebbero essere supportate le chiamate protette.

Le chiamate protette vengono effettuate mediante la procedura seguente:

1. Un utente avvia la chiamata da un telefono protetto (modalità di protezione attivata).

2. Sullo schermo del telefono viene visualizzata l'icona di protezione . Questa icona indica che il telefono è configurato per le chiamate protette, anche se ciò non garantisce che anche l'altro telefono connesso sia protetto.
3. Se la chiamata viene connessa a un altro telefono protetto, viene riprodotta una tonalità di sicurezza per indicare che la conversazione è crittografata e protetta su entrambi i lati. Se la chiamata viene connessa a un telefono non protetto, non viene riprodotta nessuna tonalità di sicurezza.

Nota Le chiamate protette sono supportate per le connessioni tra due telefoni. Alcune funzioni, come ad esempio Chiamata in conferenza, Linee condivise e Mobilità interni telefonici, non sono disponibili sui telefoni protetti se sono configurate le chiamate protette.

Solo i telefoni protetti possono riprodurre i toni indicativi protetti o non protetti. I telefoni non protetti non possono riprodurre alcun tono. Se lo stato complessivo della chiamata cambia mentre la chiamata è in corso, cambia anche il tono indicativo e il telefono protetto riproduce il tono appropriato.

Un telefono protetto riproduce o meno un tono nei casi seguenti:

- Se l'opzione Riproduci tono indicativo protetto è abilitata:
  - Quando viene stabilita una connessione end-to-end protetta e lo stato della chiamata è protetto, sul telefono viene riprodotto il tono che indica che si tratta di una chiamata protetta (tre segnali acustici prolungati, interrotti da pause).
  - Quando viene stabilita una connessione end-to-end non protetta e lo stato della chiamata è non protetto, sul telefono viene riprodotto il tono che indica che si tratta di una chiamata non protetta (sei brevi segnali acustici, interrotti da pause brevi).

Se l'opzione Riproduci tono indicativo protetto è disabilitata, non viene riprodotto alcun tono.

Fornitura della crittografia per l'Inclusione

Quando vengono effettuate delle conferenze, Cisco Unified Communications Manager verifica lo stato di protezione del telefono e modifica l'indicazione di protezione della conferenza o blocca il completamento della chiamata per mantenere integrità e protezione nel sistema.

Gli utenti non possono aggiungersi a una chiamata crittografata se il telefono in uso per l'inclusione non è configurato per la crittografia. Se in questo caso il processo di inclusione non riesce, sul telefono in cui è stato avviato tale processo viene riprodotto un tono di riordino (occupato rapido).

Se il telefono dell'utente che ha avviato la conferenza è configurato per la crittografia, l'utente che ha avviato il processo di inclusione può unirsi a una chiamata non protetta dal telefono crittografato. In seguito all'inclusione, Cisco Unified Communications Manager classifica la chiamata come non protetta.

Se il telefono dell'utente che ha avviato la conferenza è configurato per la crittografia, l'utente che ha avviato il processo di inclusione può unirsi a una chiamata crittografata e sul telefono viene indicato che la chiamata è crittografata.

Protezione WLAN

Dal momento che tutti i dispositivi WLAN all'interno della copertura possono ricevere tutto il traffico WLAN, la protezione delle comunicazioni vocali sulle reti WLAN assume un'importanza critica. Per garantire che

utenti non autorizzati non manipolino o intercettino il traffico vocale, l'architettura per la sicurezza SAFE di Cisco supporta gli AP del telefono IP Cisco e di Cisco Aironet. Per ulteriori informazioni sulla protezione sulle reti, consultare http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

La soluzione di telefonia IP Cisco Wireless offre protezione sulla rete wireless in grado di impedire accessi non autorizzati e comunicazioni compromesse tramite i seguenti metodi di autenticazione supportati dal telefono IP wireless di Cisco:

- Autenticazione aperta: tutti i dispositivi wireless possono richiedere l'autenticazione in un sistema aperto. L'AP che riceve la richiesta può concedere l'autenticazione a tutti i richiedenti o soltanto ai richiedenti presenti sull'elenco degli utenti. La comunicazione tra il dispositivo wireless e l'AP potrebbe non essere crittografata o i dispositivi possono utilizzare le chiavi WEP (Wired equivalent privacy) per fornire protezione. I dispositivi che utilizzano esclusivamente le chiavi WEP tentano di autenticarsi con un AP in cui viene utilizzato il metodo WEP.
- Autenticazione EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling): questa architettura di protezione client/server crittografa le transazioni EAP all'interno di un tunnel TLS (Transport Level Security) tra l'AP e il server RADIUS come ad esempio il server ACS (Access Control Server) di Cisco.

  Il tunnel TLS utilizza le credenziali di accesso protetto (PAC, Protected Access Credential) per l'autenticazione tra il client (telefono) e il server RADIUS. Il server invia un ID di autorità (AID) al client (telefono) che a sua volta seleziona le credenziali PAC appropriate. Il client (telefono) restituisce una chiave PAC-Opaque al server RADIUS. Il server decrittografa la chiave PAC con la chiave primaria. In entrambi gli endpoint è adesso presente la chiave PAC ed è stato creato un tunnel TLS. EAP-FAST supporta il provisioning PAC automatico, ma occorre abilitarlo sul server RADIUS.

Nota Per impostazione predefinita, la scadenza della chiave PAC sul server ACS di Cisco è impostata su una settimana. Se sul telefono è presente una chiave PAC scaduta, l'autenticazione con il server RADIUS impiega più tempo perché il telefono deve ottenere una nuova chiave PAC. Per evitare ritardi legati al provisioning della chiave PAC, impostarne la scadenza su almeno 90 giorni sul server ACS o RADIUS.

- Autenticazione EAP-TLS (Extensible Authentication Protocol-Transport Layer Security): per EAP-TLS è necessario disporre di un certificato client per l'autenticazione e l'accesso alla rete. Per EAP-TLS su connessioni con cavo, il certificato client può essere il MIC del telefono o un LSC. LSC è il certificato di autenticazione client consigliato per EAP-TLS su connessioni con cavo.
- Protected Extensible Authentication Protocol (PEAP): schema proprietario di Cisco di autenticazione reciproca basata su password tra il client (telefono) e il server RADIUS. Il telefono IP Cisco può utilizzare il protocollo PEAP per l'autenticazione con la rete wireless. Sono supportati entrambi i metodi di autenticazione PEAP-MSCHAPV2 e PEAP-GTC.

Gli schemi di autenticazione riportati di seguito utilizzano il server RADIUS per la gestione delle chiavi di autenticazione:

- WPA/WPA2: utilizza le informazioni sul server RADIUS per generare delle chiavi univoche per l'autenticazione. Dal momento che tali chiavi vengono generate sul server RADIUS centralizzato, il metodo WPA/WPA2 fornisce più protezione rispetto alle chiavi WPA già condivise memorizzate sull'AP e sul telefono.

- Roaming veloce protetto: utilizza le informazioni sul server RADIUS e sul server di dominio wireless (WDS) per la gestione e l'autenticazione delle chiavi. Il server WDS crea una cache delle credenziali di protezione per i dispositivi client abilitati per CCKM per una nuova autenticazione rapida e protetta. Il telefono IP Cisco serie 8800 supporta 802.11r (FT). Per consentire il roaming veloce protetto, sono supportati sia 11r (FT) che CCKM. Tuttavia, Cisco consiglia di utilizzare il metodo 802.11 r (FT).

Con i metodi WPA/WPA2 e CCKM, le chiavi di crittografia non vengono immesse nel telefono, ma vengono derivate automaticamente tra il telefono e l'AP. Tuttavia, è necessario immettere su ciascun telefono il nome utente e la password EAP utilizzati per l'autenticazione.

Per garantire la protezione del traffico vocale, il telefono IP Cisco supporta i meccanismi WEP, TKIP e AES (Advanced Encryption Standards) per la crittografia. Se questi meccanismi vengono utilizzati per la crittografia, i pacchetti SIP di segnalazione e i pacchetti RTP (Real-Time Transport Protocol) vengono crittografati tra l'AP e il telefono IP Cisco.

WEP

Con l'uso di WEP nella rete wireless, l'autenticazione si verifica a livello di AP tramite l'uso dell'autenticazione aperta o con chiave condivisa. Per stabilire delle connessioni corrette, la chiave WEP impostata sul telefono deve corrispondere alla chiave WEP configurata sull'AP. Il telefono IP Cisco supporta le chiavi WEP con crittografia a 40 bit o a 128 bit e che rimangono statiche sul telefono e l'AP.

Le autenticazioni EAP e CCKM possono utilizzare le chiavi WEP per la crittografia. Il server RADIUS gestisce la chiave WEP e trasmette una chiave univoca all'AP in seguito all'autenticazione per la crittografia di tutti i pacchetti voce; di conseguenza, tali chiavi WEP possono cambiare a ogni autenticazione.

TKIP

WPA e CCKM utilizzano la crittografia TKIP che presenta numerosi miglioramenti rispetto alla crittografia WEP. La crittografia TKIP fornisce cifratura di chiave per ogni pacchetto e vettori di inizializzazione (IV) più lunghi che aumentano la protezione della crittografia. Inoltre, il controllo dell'integrità dei messaggi (MIC, Message Integrity Check) garantisce che i pacchetti crittografati non vengano alterati. La crittografia TKIP rimuove la prevedibilità delle chiavi WEP di cui si servono gli utenti non autorizzati per decifrare tali chiavi.

AES

Un metodo di crittografia utilizzato per l'autenticazione WPA2. Questo National Standard di crittografia utilizza un algoritmo simmetrico con la stessa chiave per la crittografia e la decrittografia. Il metodo AES utilizza la crittografia CBC (Cipher Blocking Chain) a 128 bit, che supporta le dimensioni di chiave di minimo 128, 192 e 256 bit. Il telefono IP Cisco supporta la dimensione di chiave di 256 bit.

Nota Il telefono IP Cisco non supporta il protocollo CKIP (Cisco Key Integrity Protocol) con CMIC.

Gli schemi di autenticazione e crittografia vengono impostati all'interno della LAN wireless. Le VLAN vengono configurate nella rete e sull'AP e specificano diverse combinazioni di autenticazione e crittografia. Un SSID effettua l'associazione con una VLAN e lo schema di autenticazione e crittografia specifico. Per un'autenticazione corretta dei dispositivi client wireless, è necessario configurare gli stessi SSID con i relativi schemi di autenticazione e crittografia sugli AP e sul telefono IP Cisco.

Alcuni schemi di autenticazione richiedono tipi specifici di crittografia. Per ulteriore protezione, con l'autenticazione aperta è possibile utilizzare la chiave WEP statica per la crittografia. Ma se si utilizza l'autenticazione con chiave condivisa, è necessario impostare una chiave WEP statica per la crittografia e configurare la chiave WEP sul telefono.

Nota

- Se si utilizza la chiave WPA o WPA2 già condivisa, tale chiave deve essere impostata staticamente sul telefono. Queste chiavi devono corrispondere a quelle presenti sull'AP.
- Il telefono IP Cisco non supporta la negoziazione EAP; per utilizzare la modalità EAP-FAST, è necessario specificarla.

Nella tabella seguente viene fornito un elenco degli schemi di autenticazione e crittografia configurati sugli AP Cisco Aironet e supportati dal telefono IP Cisco. Nella tabella viene illustrata l'opzione di configurazione della rete del telefono corrispondente alla configurazione dell'AP.

Tabella 28: Schemi di autenticazione e crittografia

Configurazione telefono IP Cisco	**Configurazione AP**			
Modalità Protezione	Sicurezza	Gestione delle chiavi	Crittografia	Roaming veloce
Nessuno	Nessuno	Nessuno	Nessuno	N/D
WEP	WEP statica	Statica	WEP	N/D
PSK	PSK	WPA	TKIP	Nessuna
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM
PEAP-GTC	PEAP-GTC	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT, CCKM

Per ulteriori informazioni sulla configurazione degli schemi di autenticazione e crittografia sugli AP, consultare la *Guida di configurazione di Cisco Aironet* relativa al modello e alla versione in uso disponibile all'URL seguente:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

Impostazione della modalità di autenticazione

Per selezionare la modalità di autenticazione per questo profilo, attenersi alla procedura seguente:

Procedura

Passaggio 1 Selezionare il profilo di rete che si desidera configurare.

Passaggio 2 Selezionare la modalità di autenticazione.

Nota A seconda della modalità selezionata, è necessario configurare delle opzioni aggiuntive in Protezione wireless o Crittografia wireless. Per ulteriori informazioni, vedere Protezione WLAN, a pagina 97.

Passaggio 3 Fare clic su **Salva** per applicare la modifica.

Credenziali di protezione wireless

Se sulla rete vengono utilizzati i metodi EAP-FAST e PEAP per l'autenticazione dell'utente, è necessario configurare il nome utente e la password se richiesti sul servizio RADIUS (Remote Authentication Dial-In User Service) e sul telefono.

Nota Se all'interno della rete vengono utilizzati dei domini, è necessario immettere il nome utente insieme al nome del dominio nel formato *dominio/nome utente*.

Le seguenti azioni potrebbero cancellare la password Wi-Fi esistente:

- Immissione di un ID utente o di una password non validi
- Installazione di un certificato principale CA non valido o scaduto se il tipo EAP è impostato su PEAP-MSCHAPV2 o PEAP-GTC
- Disabilitazione del tipo EAPa sul server RADIUS utilizzato dal telefono prima di impostare il nuovo tipo di EAP sul telefono

Per modificare i tipi EAP, eseguire le seguenti operazioni nell'ordine indicato:

- Abilitare i nuovi tipi EAP sul server RADIUS.
- Modificare il tipo EAP su un telefono impostando il nuovo tipo EAP.

Mantenere il tipo EAP corrente configurato sul telefono fino a quando sul server RADIUS non è abilitato il nuovo tipo EAP. Una volta che il nuovo tipo di EP è abilitato sul server RADIUS, è possibile modificare il tipo EAP del telefono. Una volta che tutti i telefoni sono stati modificati impostando il nuovo tipo EAP, se si desidera, è possibile disabilitare il tipo EAP precedente.

Impostazione del nome utente e della password

Per immettere o modificare il nome utente o la password del profilo di rete, è necessario utilizzare lo stesso nome utente e la stessa stringa di password configurati sul server RADIUS. La lunghezza massima del nome utente o della password è di 64 caratteri.

Per impostare il nome utente e la password nell'area Credenziali di protezione wireless, attenersi alla procedura seguente:

Procedura

Passaggio 1	Selezionare un profilo di rete.
Passaggio 2	Nel campo Nome utente, immettere il nome utente di rete per il profilo.
Passaggio 3	Nel campo Password, immettere la password di rete per il profilo.
Passaggio 4	Fare clic su **Salva** per applicare la modifica.

Configurazione chiave già condivisa

Utilizzare le seguenti sezioni per impostare le chiavi già condivise.

Formati della chiave già condivisa

Il telefono IP Cisco supporta i formati ASCII ed esadecimali. Durante l'impostazione di una chiave WPA già condivisa, è necessario utilizzare uno di questi formati:

Esadecimale

Per le chiavi esadecimali, immettere 64 cifre esadecimali (da 0 a 9 e da A a F); ad esempio AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C.

ASCII

Per le chiavi ASCII, immettere una stringa di caratteri in cui siano utilizzati i numeri da 0 a 9 e i caratteri da A a Z (maiuscoli e minuscoli), inclusi i simboli, di lunghezza compresa tra 8 e 63 caratteri; ad esempio GREG12356789ZXYW.

Impostazione di PSK

Per impostare un PSK nell'area delle credenziali wireless, attenersi alla procedura seguente:

Procedura

Passaggio 1	Selezionare il profilo di rete che abilita la chiave WPA o la chiave WPA2 già condivise.
Passaggio 2	Nell'area Tipo di chiave, immettere la chiave appropriata.
Passaggio 3	Immettere una stringa ASCII o delle cifre esadecimali nel campo Passphrase/Chiave già condivisa.
Passaggio 4	Fare clic su **Salva** per applicare la modifica.

Crittografia wireless

Se sulla rete wireless viene utilizzata la crittografia WEP e la modalità di autenticazione viene impostata su Aperta + WEP, è necessario immettere una chiave WEP ASCII o esadecimale.

Le chiavi WEP impostate sul telefono devono corrispondere alle chiavi WEP assegnate all'AP. Il telefono IP Cisco e i punti di accesso Cisco Aironet supportano le chiavi di crittografia a 40 e 128 bit.

Formati della chiave WEP

Per l'impostazione di una chiave WEP, è necessario utilizzare uno dei formati seguenti:

Esadecimale

Per le chiavi esadecimali, utilizzare una delle dimensioni di chiave seguenti:

40 bit

Immettere una stringa della chiave di crittografia a 10 cifre in cui siano utilizzate delle cifre esadecimali (da 0 a 9 e da A a F); ad esempio: ABCD123456.

128 bit

Immettere una stringa della chiave di crittografia a 26 cifre in cui siano utilizzate delle cifre esadecimali (da 0 a 9 e da A a F); ad esempio: AB123456789CD01234567890EF.

ASCII

Per le chiavi ASCII, immettere una stringa di caratteri in cui siano utilizzati i numeri da 0 a 9 e i caratteri da A a Z (maiuscoli e minuscoli) e tutti i simboli, con una delle dimensioni di chiave seguenti:

40 bit

Immettere una stringa a 5 caratteri, ad esempio GREG5.

128 bit

Immettere una stringa a 13 caratteri, ad esempio GREGSSECRET13.

Impostazione delle chiavi WEP

Per impostare le chiavi WEP, attenersi alla procedura seguente.

Procedura

Passaggio 1 Scegliere il profilo di rete in cui viene utilizzato il metodo Aperto+WEP o Condiviso+WEP.

Passaggio 2 Nell'area Tipo di chiave, immettere la chiave appropriata.

Passaggio 3 Nell'area Dimensione chiave, scegliere una delle seguenti lunghezze di stringa dei caratteri:

- **40**
- **128**

Passaggio 4 Nel campo Chiave di crittografia, immettere la stringa di chiave appropriata in base al tipo e alla dimensione della chiave selezionati. Consultare Formati della chiave WEP, a pagina 103.

Passaggio 5 Fare clic su **Salva** per applicare la modifica.

Esportazione di un certificato CA dal server ACS tramite i Servizi certificati Microsoft

Esportare il certificato CA dal server ACS. Per ulteriori informazioni, consultare la documentazione su CA e RADIUS.

Certificato installato dal produttore (MIC)

Cisco ha incluso un certificato MIC (Manufacture Installed Certificate) nel telefono.

Durante l'autenticazione EAP-TLS, il server ACS deve verificare l'attendibilità del telefono che a sua volta deve verificare l'attendibilità del server ACS.

Per verificare il MIC, è necessario esportare il certificato principale di produzione e il certificato dell'autorità certificativa (CA) di produzione dal telefono IP Cisco e installarli sul server ACS di Cisco. Questi due certificati sono parte della catena di certificati attendibili utilizzata dal server ACS di Cisco per verificare il certificato MIC.

Per verificare il certificato ACS di Cisco, è necessario esportare e installare sul telefono un certificato subordinato attendibile (se presente) e un certificato principale (creato da un'autorità certificativa) sul server ACS di Cisco. Questi certificati sono parte della catena di certificati attendibili utilizzata dal server ACS di Cisco per verificare l'attendibilità del certificato.

Certificato installato dall'utente

Per utilizzare un certificato installato dall'utente, viene generata una CSR (Certificate Signing Request) e inviata alla CA per l'approvazione. Un certificato utente può anche essere generato dall'autorità certificativa senza un rappresentante del servizio.

Durante l'autenticazione EAP-TLS, il server ACS verifica l'attendibilità del telefono che a sua volta verifica l'attendibilità del server ACS.

Per verificare l'autenticità del certificato installato dall'utente, è necessario installare sul server ACS di Cisco un certificato subordinato attendibile (se presente) e un certificato principale dall'autorità certificativa che ha approvato il certificato utente. Questi certificati sono parte della catena di certificati attendibili utilizzata per verificare l'attendibilità del certificato installato dall'utente.

Per verificare il certificato ACS di Cisco, esportare sul server ACS di Cisco un certificato subordinato attendibile (se presente) e un certificato principale (creato da un'autorità certificativa); i certificati esportati vengono quindi installati sul telefono. Questi certificati sono parte della catena di certificati attendibili utilizzata dal server ACS di Cisco per verificare l'attendibilità del certificato.

Installazione dei certificati di autenticazione EAP-TLS

Per installare i certificati di autenticazione per EAP-TLS, attenersi alla procedura seguente.

Procedura

Passaggio 1 Dalla pagina Web del telefono, impostare la data e l'ora di Cisco Unified Communications Manager sul telefono.

Passaggio 2 Se si utilizza il certificato MIC (Manufacturing Installed Certificate):

a) Dalla pagina Web del telefono, esportare il certificato principale CA e il certificato CA di produzione.
b) Da Internet Explorer, installare i certificati sul server ACS di Cisco e modificare la Trust List.
c) Importare il certificato CA nel telefono.

Per ulteriori informazioni, consultare:

- Esportazione e installazione dei certificati sul server ACS, a pagina 105
- Esportazione di un certificato CA da ISE tramite i Servizi certificati Microsoft, a pagina 106

Passaggio 3 Mediante lo strumento di configurazione ACS, impostare l'account utente.

Per ulteriori informazioni, consultare:

- Impostazione dell'account utente ACS e installazione del certificato, a pagina 108
- *Guida per l'utente di Cisco Secure ACS per Windows* (http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html)

Impostazione di data e ora

Il metodo EAP-TLS utilizza l'autenticazione basata su certificato che richiede l'impostazione corretta dell'orologio interno del telefono IP Cisco. La data e l'ora del telefono possono cambiare quando il telefono viene registrato su Cisco Unified Communications Manager.

Nota Se è necessario un nuovo certificato di autenticazione del server e l'ora locale è indietro rispetto al fuso orario GMT (Greenwich Mean Time), la convalida del certificato di autenticazione potrebbe non riuscire. Cisco consiglia di impostare la data e l'ora locali in avanti rispetto al fuso orario GMT.

Per impostare il telefono sulla data e l'ora locali corrette, attenersi alla procedura seguente.

Procedura

Passaggio 1 Selezionare **Data e ora** nel riquadro di navigazione a sinistra.

Passaggio 2 Se l'impostazione nel campo Data e ora telefono correnti è diversa da quella del campo Data e ora locali, fare clic su **Imposta telefono alla data e ora locali**.

Passaggio 3 Fare clic su **Riavvio telefono**, quindi su **OK**.

Esportazione e installazione dei certificati sul server ACS

Per utilizzare il certificato MIC, esportare il certificato principale di produzione e il certificato CA di produzione e installarli sul server ACS di Cisco.

Per esportare il certificato principale di produzione e il certificato CA di produzione sul server ACS, attenersi alla procedura seguente.

Procedura

Passaggio 1 Dalla pagina Web del telefono, selezionare **Certificati**.

Passaggio 2 Fare clic su **Esporta** accanto al certificato principale di produzione.

Passaggio 3 Salvare il certificato e copiarlo sul server ACS.

Passaggio 4 Ripetere i passaggi 1 e 2 per il certificato CA di produzione.

Passaggio 5 Dalla pagina Configurazione del sistema del server ACS, immettere il percorso di file per ciascun certificato e installare i certificati.

Nota Per ulteriori informazioni sull'uso dello strumento di configurazione ACS, consultare la guida in linea di ACS o la *Guida per l'utente di Cisco Secure ACS per Windows* (http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html).

Passaggio 6 Tramite la pagina Modifica CTL (Certificate Trust List), aggiungere i certificati che devono essere considerati attendibili da ACS.

Metodi di esportazione del certificato ACS

A seconda del tipo di certificato esportato dal server ACS, utilizzare uno dei metodi seguenti:

- Per esportare il certificato CA dal server ACS che ha firmato il certificato installato dall'utente o il certificato ACS, consultare Esportazione di un certificato CA da ISE tramite i Servizi certificati Microsoft, a pagina 106.
- Per esportare il certificato CA dal server ACS in cui viene utilizzato un certificato autofirmato, consultare Esportazione di un certificato CA dal server ACS tramite Internet Explorer, a pagina 106.

Esportazione di un certificato CA da ISE tramite i Servizi certificati Microsoft

Utilizzare questo metodo per esportare un certificato CA dal server ISE che ha firmato il certificato installato dall'utente o il certificato ISE.

Per esportare il certificato CA tramite la pagina Web dei Servizi certificati Microsoft, attenersi alla procedura seguente.

Procedura

Passaggio 1 Dalla pagina Web dei Servizi certificati Microsoft, selezionare **Scarica un certificato CA, la catena di certificati o un CRL**.

Passaggio 2 Nella pagina successiva, evidenziare il certificato CA corrente nella casella di testo, scegliere DER in Metodo di codifica, quindi fare clic su **Scarica certificato CA**.

Passaggio 3 Salvare il certificato CA.

Esportazione di un certificato CA dal server ACS tramite Internet Explorer

Utilizzare questo metodo per esportare un certificato CA dal server ACS in cui viene utilizzato un certificato autofirmato.

Per esportare i certificati dal server ACS tramite Internet Explorer, attenersi alla procedura seguente.

Procedura

Passaggio 1	Da Internet Explorer, selezionare **Strumenti** > **Opzioni Internet**, quindi fare clic sulla scheda Contenuto.
Passaggio 2	In Certificati, fare clic su **Certificati**, quindi sulla scheda Autorità di certificazione radice attendibili.
Passaggio 3	Evidenziare il certificato principale e premere **Esporta**. Viene visualizzata la procedura guidata per l'esportazione del certificato.
Passaggio 4	Fare clic su **Avanti**.
Passaggio 5	Nella finestra successiva, selezionare **X.509 binario codificato DER (.CER)** e fare clic su **Avanti**.
Passaggio 6	Specificare un nome per il certificato e fare clic su **Avanti**.
Passaggio 7	Salvare il certificato CA da installare sul telefono.

Richiesta e importazione del certificato installato dall'utente

Per richiedere e installare il certificato sul telefono, attenersi alla procedura seguente.

Procedura

Passaggio 1	Dalla pagina Web del telefono, selezionare il profilo di rete tramite EAP-TLS e selezionare Installato dall'utente nel campo Certificato EAP-TLS.
Passaggio 2	Fare clic su **Certificati**. Nella pagina Installazione certificato utente, il campo Nome comune deve corrispondere al nome utente nel server ACS. **Nota** Se si desidera, è possibile modificare il campo Nome comune. Assicurarsi che il nome utente immesso in tale campo corrisponda a quello immesso nel server ACS. Consultare Impostazione dell'account utente ACS e installazione del certificato, a pagina 108.
Passaggio 3	Immettere le informazioni da visualizzare sul certificato e fare clic su **Invia** per generare la richiesta di firma del certificato (CSR).

Installazione del certificato principale del server di autenticazione

Per installare il certificato principale del server di autenticazione, attenersi alla procedura seguente.

Procedura

Passaggio 1	Esportare il certificato principale del server di autenticazione dal server ACS. Consultare Metodi di esportazione del certificato ACS, a pagina 106.
Passaggio 2	Andare alla pagina Web del telefono e selezionare **Certificati**.
Passaggio 3	Fare clic su **Importa** accanto al certificato principale del server di autenticazione.
Passaggio 4	Riavviare il telefono.

Impostazione dell'account utente ACS e installazione del certificato

Per impostare il nome dell'account utente e installare il certificato principale MIC per il telefono sul server ACS, attenersi alla procedura seguente.

Nota Per ulteriori informazioni sull'uso dello strumento di configurazione ACS, consultare la guida in linea di ACS o la *Guida per l'utente di Cisco Secure ACS per Windows*.

Procedura

Passaggio 1 Dalla pagina Impostazione utente dello strumento di configurazione di ACS, creare un nome dell'account utente del telefono, se non è stato ancora configurato.

In genere, la parte finale del nome utente include l'indirizzo MAC del telefono. Per EAP-TLS non è necessaria nessuna password.

Nota Assicurarsi che il nome utente corrisponda a quello immesso nel campo Nome comune nella pagina Installazione certificato utente. Consultare Richiesta e importazione del certificato installato dall'utente, a pagina 107.

Passaggio 2 Nella pagina Configurazione del sistema, nella sezione EAP-TLS, attivare questi campi:

- **Consenti EAP-TLS**
- **Confronto NC certificato**

Passaggio 3 Nella pagina Impostazione autorità certificativa ACS, aggiungere il certificato principale di produzione e il certificato CA di produzione al server ACS.

Passaggio 4 Attivare sia il certificato principale di produzione, sia il certificato CA di produzione nella Trust List del server ACS.

Configurazione PEAP

Il protocollo PEAP (Protected Extensible Authentication Protocol) utilizza i certificati di chiave pubblica lato server per l'autenticazione dei client tramite la creazione di un tunnel SSL/TLS crittografato tra il client e il server di autenticazione.

Il telefono IP Cisco 8865 supporta solo un certificato del server che può essere installato tramite SCEP o con il metodo di installazione manuale, ma non con entrambi. Il telefono non supporta il metodo TFTP per l'installazione del certificato.

Nota È possibile abilitare la convalida del server di autenticazione importando il certificato del server di autenticazione.

Operazioni preliminari

Prima di configurare l'autenticazione PEAP per il telefono, assicurarsi che siano rispettati i seguenti requisiti di Cisco Secure ACS:

- Il certificato principale ACS deve essere installato.
- È inoltre possibile installare un certificato per abilitare la convalida del server per PEAP. Tuttavia, se non è installato un certificato del server, la convalida del server è abilitata.
- L'impostazione Consenti EAP-MSCHAPv2 deve essere abilitata.
- L'account utente e la password devono essere configurati.
- Per l'autenticazione della password, è possibile utilizzare il database ACS locale o un database esterno (come ad esempio un database Windows o LDAP).

Abilitazione dell'autenticazione PEAP

Procedura

Passaggio 1	Dalla pagina Web della configurazione del telefono, selezionare PEAP come modalità di autenticazione.
Passaggio 2	Immettere un nome utente e una password.

Protezione LAN wireless

I telefoni Cisco che supportano il Wi-Fi hanno più requisiti di protezione e richiedono una configurazione aggiuntiva. Questa procedura aggiuntiva prevede l'installazione di certificati e l'impostazione della protezione sui telefoni e su Cisco Unified Communications Manager.

Per ulteriori informazioni, consultare la *Guida alla protezione di Cisco Unified Communications Manager*.

Pagina Amministrazione del telefono IP Cisco

I telefoni Cisco che supportano il Wi-Fi presentano delle pagine Web speciali diverse dalle pagine degli altri telefoni. Tali pagine Web speciali si utilizzano per la configurazione della protezione del telefono in assenza di un Simple Certificate Enrollment Protocol (SCEP). Utilizzare queste pagine per installare manualmente certificati di sicurezza su un telefono, per scaricare un certificato di sicurezza o per configurare manualmente la data e l'ora del telefono.

Queste pagine Web mostrano anche le stesse informazioni presenti su altre pagine Web del telefono, incluse le informazioni sul dispositivo, l'impostazione di rete, i registri e le informazioni statistiche.

Argomenti correlati

Pagina Web del telefono IP Cisco, a pagina 237

Configurazione della pagina di amministrazione per il telefono

La pagina Web di amministrazione è abilitata per impostazione predefinita e la password è Cisco. Tuttavia, se un telefono viene registrato su Cisco Unified Communications Manager, è necessario abilitare la pagina Web di amministrazione e configurare una nuova password.

Abilitare questa pagina Web e impostare le credenziali di accesso prima di utilizzarla per la prima volta dopo la registrazione del telefono.

Una volta abilitata, la pagina Web di amministrazione è accessibile dalla porta HTTPS 8443 (**`https://x.x.x.x:8443`**, dove x.x.x. x è l'indirizzo IP del telefono).

Prima di iniziare

Scegliere una password prima di abilitare la pagina Web di amministrazione. La password può essere una qualsiasi combinazione di lettere o numeri, ma deve contenere da 8 a 127 caratteri.

Il nome utente è impostato in modo permanente su admin.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono.

Passaggio 3 Nella sezione **Layout configurazione specifica prodotto**, impostare il parametro **Amministratore Web** su **Abilitato**.

Passaggio 4 Nel campo **Password amministratore** immettere una password.

Passaggio 5 Selezionare **Salva** e fare clic su **OK**.

Passaggio 6 Selezionare **Applica configurazione** e fare clic su **OK**.

Passaggio 7 Riavviare il telefono.

Accedere alla pagina Web di amministrazione del telefono

Quando si desidera accedere alle pagine Web di amministrazione, è necessario specificare la porta di amministrazione.

Procedura

Passaggio 1 Richiedere l'indirizzo IP del telefono:

- In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono** e individuare il telefono. Sui telefoni registrati in Cisco Unified Communications Manager viene visualizzato l'indirizzo IP nella finestra **Cerca ed elenca telefoni** e in cima alla finestra **Configurazione telefono**.
- Sul telefono, premere **Applicazioni** , scegliere **Informazioni telefono**, quindi scorrere fino al campo dell'indirizzo IPv4.

Passaggio 2 Aprire un browser Web e immettere il seguente URL, dove *indirizzo_IP* è l'indirizzo IP del telefono IP Cisco:

`https://<IP_address>:8443`

Passaggio 3 Immettere la password nel campo Password.

Passaggio 4 Fare clic su **Submit**.

Installazione di un certificato utente dalla pagina Web di amministrazione del telefono

Se SCEP (Simple Certificate Enrollment Protocol) non è disponibile, è possibile installare manualmente un certificato utente sul telefono.

È possibile utilizzare il certificato MIC (Manufacturing Installed Certificate) preinstallato come certificato utente per EAP-TLS.

Dopo aver installato il certificato utente, è necessario aggiungerlo alla Trust List del server RADIUS.

Prima di iniziare

Prima di installare un certificato utente per un telefono, è necessario disporre di quanto segue:

- Un certificato utente salvato sul computer. Il certificato deve essere in formato PKCS #12.
- La password di estrazione del certificato.

Procedura

Passaggio 1	Dalla pagina Web di amministrazione del telefono, selezionare **Certificati**.
Passaggio 2	Individuare il campo Installazione utente campo e fare clic su **Installa**.
Passaggio 3	Selezionare il certificato sul PC.
Passaggio 4	Nel campo **Password di estrazione**, immettere la password di estrazione del certificato.
Passaggio 5	Fare clic su **Carica**.
Passaggio 6	Al termine del caricamento, riavviare il telefono.

Installazione di un certificato del server di autenticazione dalla pagina Web di amministrazione del telefono

Se SCEP (Simple Certificate Enrollment Protocol) non è disponibile, è possibile installare manualmente un certificato del server di autenticazione sul telefono.

Per EAP-TLS è necessario installare il certificato principale dell'Autorità di certificazione che ha emesso il certificato del server RADIUS.

Prima di iniziare

Prima di installare un certificato su un telefono, è necessario disporre di un certificato del server di autenticazione salvato sul computer. Il certificato deve essere codificato in PEM (in base 64) o DER.

Procedura

Passaggio 1	Dalla pagina Web di amministrazione del telefono, selezionare **Certificati**.
Passaggio 2	Individuare il campo **CA server di autenticazione (pagina Web amministratore)** e fare clic su **Installa**.
Passaggio 3	Selezionare il certificato sul PC.
Passaggio 4	Fare clic su **Carica**.
Passaggio 5	Al termine del caricamento, riavviare il telefono.

Se si installa più di un certificato, installare tutti i certificati prima di riavviare il telefono.

Rimuovere manualmente un certificato di protezione dalla pagina Web di amministrazione del telefono

Se il protocollo SCEP (Simple Certificate Enrollment Protocol) non è disponibile, è possibile rimuovere manualmente un certificato utente dal telefono.

Procedura

Passaggio 1	Dalla pagina Web di amministrazione del telefono, selezionare **Certificati**.
Passaggio 2	Individuare il certificato nella pagina **Certificati**.
Passaggio 3	Fare clic su **Elimina**.
Passaggio 4	Una volta completata la procedura di eliminazione, riavviare il telefono.

Impostazione manuale della data e ora del telefono

Con l'autenticazione basata su certificato, il telefono deve visualizzare la data e l'ora corrette. Il server di autenticazione verifica la data e l'ora del telefono rispetto alla data di scadenza del certificato. Se la data e l'ora del telefono e del server non corrispondono, il telefono smette di funzionare.

Se il telefono non riceve le informazioni corrette dalla rete, utilizzare questa procedura per configurare manualmente la data e l'ora del telefono.

Procedura

Passaggio 1	Dalla pagina Web di amministrazione del telefono, scorrere fino alla voce **Data e ora**.
Passaggio 2	Eseguire una delle seguenti opzioni: • Fare clic su **Imposta telefono alla data e ora locali** per sincronizzare il telefono con un server locale. • Nei campi **Specifica data e ora**, selezionare il mese, il giorno, l'anno, le ore, i minuti e i secondi utilizzando i menu e fare clic su **Imposta telefono alla data e l'ora specificati**.

Configurazione SCEP

Il Simple Certificate Enrollment Protocol (SCEP) rappresenta lo standard per la fornitura e il rinnovo automatici di certificati. Evita l'installazione manuale dei certificati sui telefoni.

Impostazione dei parametri della configurazione specifica del prodotto SCEP

È necessario configurare i seguenti parametri SCEP nella pagina Web telefono:

- Indirizzo IP Agente registrazione
- Firma digitale SHA-1 o SHA-256 oppure certificato CA principale per il server SCEP

L'autorità di registrazione Cisco IOS viene utilizzata come proxy per il server SCEP. Il client SCEP sul telefono utilizza i parametri scaricati da Cisco Unified Communications Manager. Dopo aver configurato i parametri, il telefono invia una richiesta `SCEP getcs` all'Autorità di registrazione e il certificato CA principale viene convalidato utilizzando l'impronta digitale predefinita.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.
Passaggio 2	Individuare il telefono.
Passaggio 3	Scorrere fino all'area **Layout configurazione specifica del prodotto**.
Passaggio 4	Selezionare la casella di controllo **Server SCEP WLAN** per attivare il parametro SCEP.
Passaggio 5	Selezionare la casella di controllo **Impronta digitale CA radice WLAN (SHA256 o SHA1)** per attivare il parametro SCEP QED.

Supporto di SCEP (Simple Certificate Enrollment Protocol)

Se si utilizza un server SCEP (Simple Certificate Enrollment Protocol), il server è in grado di gestire automaticamente i certificati del server e degli utenti. Sul server SCEP, configurare l'agente di registrazione (RA) di SCEP in modo per:

- Fungere da trust point per l'infrastruttura a chiave pubblica (PKI)
- Fungere da agente di registrazione (RA) per l'infrastruttura a chiave pubblica (PKI)
- Eseguire l'autenticazione del dispositivo utilizzando un server RADIUS

Per ulteriori informazioni, consulta la documentazione del server SCEP.

Autenticazione 802.1X

Il telefono IP Cisco supporta l'autenticazione 802.1X.

I telefoni IP Cisco e gli switch Cisco Catalyst generalmente utilizzano il protocollo CDP (Cisco Discovery Protocol) per l'identificazione reciproca e per l'individuazione di parametri come l'allocazione VLAN e i requisiti di alimentazione in linea. Il protocollo CDP non identifica le postazioni di lavoro collegate in locale. I telefoni IP Cisco sono dotati di un meccanismo EAPOL pass-through. Questo meccanismo consente alla postazione di lavoro collegata al telefono IP Cisco di trasmettere i messaggi EAPOL all'autenticatore 802.1X sullo switch LAN. Il meccanismo pass-through garantisce che il telefono IP non agisca come switch LAN per l'autenticazione dell'endpoint dei dati prima di accedere alla rete.

I telefoni IP Cisco sono dotati inoltre di un meccanismo di disconnessione EAPOL proxy. Nel caso in cui il PC collegato in locale venga disconnesso dal telefono IP, lo switch LAN non rileva l'errore del collegamento fisico perché il collegamento tra lo switch LAN e il telefono IP viene mantenuto. Per evitare di compromettere l'integrità della rete, il telefono IP invia un messaggio di disconnessione EAPOL allo switch per conto del PC downstream, che attiva lo switch LAN allo scopo di cancellare la voce di autenticazione relativa al PC downstream.

Il supporto dell'autenticazione 802.1X richiede diversi componenti:

- Telefono IP Cisco: il telefono avvia la richiesta di accesso alla rete. I telefoni IP Cisco sono dotati di un richiedente 802.1X. Tale richiedente consente agli amministratori di rete di controllare la connettività

dei telefoni IP alle porte dello switch LAN. Per l'autenticazione della rete, nella versione corrente del richiedente 802.1X del telefono vengono utilizzate le opzioni EAP-FAST e EAP-TLS.

- Cisco Secure Access Control Server (ACS), o un altro server di autenticazione di terze parti: per autenticare il telefono, è necessario configurare il server di autenticazione e il telefono su un segreto condiviso.
- Switch Cisco Catalyst (o altri switch di terze parti): affinché possa agire come autenticatore e trasmettere i messaggi tra il telefono e il server di autenticazione, è necessario che lo switch supporti il protocollo 802.1X. Al termine dello scambio, lo switch concede o nega al telefono l'accesso alla rete.

Per configurare l'autenticazione 802.1X, è necessario effettuare i passaggi seguenti.

- Configurare gli altri componenti prima di abilitare l'autenticazione 802.1X sul telefono.
- Configurare la porta PC: lo standard 802.1X non prende in considerazione le reti VLAN e pertanto è consigliabile autenticare un solo dispositivo su una porta dello switch specifica. Tuttavia, alcuni switch (inclusi gli switch Cisco Catalyst) supportano l'autenticazione multidominio. In base alla configurazione dello switch, è possibile o meno collegare un PC alla porta PC del telefono.
  - Abilitato: se si sta utilizzando uno switch in grado di supportare l'autenticazione multidominio, è possibile abilitare la porta PC e connettervi il PC. In questo caso, i telefoni IP Cisco supportano la disconnessione EAPOL del proxy per monitorare gli scambi di autenticazione tra lo switch e il PC collegato. Per ulteriori informazioni sul supporto di IEEE 802.1X sugli switch Cisco Catalyst, consultare le guide di configurazione dello switch Cisco Catalyst all'indirizzo:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html.

  - Disabilitato: se lo switch non supporta più dispositivi conformi allo standard 802.1X sulla stessa porta, è consigliabile disabilitare la porta PC quando l'autenticazione 802.1X è abilitata. Se questa porta non viene disabilitata e successivamente si tenta di collegarvi un PC, lo switch nega l'accesso alla rete sia al telefono sia al PC.
- Configura rete VLAN vocale: dal momento che lo standard 802.1X non prende in considerazione le reti VLAN, è consigliabile configurare questa impostazione in base al tipo di supporto dello switch in uso.
  - Abilitato: se si sta utilizzando uno switch in grado di supportare l'autenticazione multidominio, è possibile continuare a utilizzare la VLAN vocale.
  - Disabilitato: se lo switch non supporta l'autenticazione multidominio, disabilitare la VLAN vocale e valutare di assegnare la porta alla rete VLAN nativa.

Accesso all'autenticazione 802.1X

Attenersi alla seguente procedura per accedere alle impostazioni dell'autenticazione 802.1X:

Procedura

Passaggio 1	Premere **Applicazioni** .
Passaggio 2	Selezionare **Impostazioni amministratore** > **Impostazione protezione** > **Autenticazione 802.1X**.
Passaggio 3	Configurare le opzioni come descritto in Opzioni di autenticazione 802.1X, a pagina 115.
Passaggio 4	Per uscire dal menu, premere **Esci**.

Opzioni di autenticazione 802.1X

Nella tabella seguente vengono descritte le opzioni di autenticazione 802.1X.

Tabella 29: Impostazioni di autenticazione 802.1X

Opzione	Descrizione	Per modificare
Autenticazione dispositivo	Determina se l'autenticazione 802.1X è abilitata: • Abilitata: il telefono utilizza l'autenticazione 802.1X per richiedere l'accesso alla rete. • Disabilitata: impostazione predefinita. Il telefono utilizza CDP per ottenere l'accesso alla VLAN e alla rete.	Consultare Impostazione del can Autenticazione dispositivo, a pag
Stato transazione	Stato: visualizza lo stato dell'autenticazione 802.1x: • Disconnesso: indica che l'autenticazione 802.1X non è configurata sul telefono. • Autenticato: indica che il telefono è autenticato. • In attesa: indica che il processo di autenticazione è in corso. Protocollo: visualizza il metodo EAP utilizzato per l'autenticazione 802.1x (può trattarsi di EAP-FAST o EAP-TLS).	Solo visualizzazione. Impossibile

Impostazione del campo Autenticazione dispositivo

Procedura

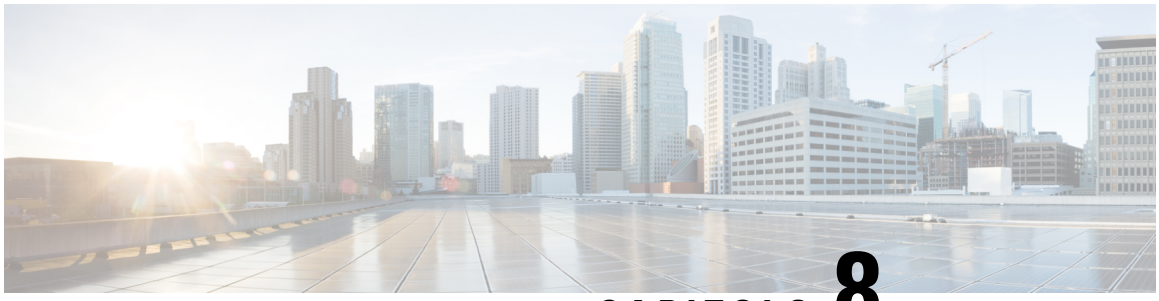
Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Impostazione protezione** > **Autenticazione 802.1X**

Passaggio 3 Impostare l'opzione Autenticazione dispositivo:

- **Sì**
- **No**

Passaggio 4 Premere **Applica**.



CAPITOLO 8

Personalizzazione del telefono IP Cisco

Suonerie personalizzate del telefono

Il telefono viene fornito con tre suonerie implementate nell'hardware: Sunshine, Chirp e Chirp1.

Cisco Unified Communications Manager fornisce inoltre un set predefinito di suonerie aggiuntive implementate nel software come file PCM (Pulse Code Modulation). I file PCM, insieme a un file XML (denominato Ringlist-wb.xml), in cui vengono descritte le opzioni dell'elenco delle suonerie disponibili sul sito, si trova all'interno della directory TFTP su ciascun server Cisco Unified Communications Manager.

Attennzione Per tutti i nomi di file viene applicata la distinzione tra lettere maiuscole e minuscole. Se si utilizza Ringlist-wb.xml come nome file, le modifiche non verranno applicate sul telefono.

Per ulteriori informazioni, consultare il capitolo "Squilli e sfondi personalizzati" della Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager per Cisco Unified Communications Manager 12.0 (1) o versioni successive.

Immagini di sfondo personalizzate

È possibile personalizzare il telefono IP Cisco con un'immagine di sfondo o uno sfondo. Gli sfondi personalizzati sono un metodo molto utilizzato per visualizzare loghi o immagini aziendali e molte organizzazioni li utilizzano per personalizzare i propri telefoni.

A partire dalla versione del firmware 12.7 (1), è possibile personalizzare lo sfondo sia sui telefoni che sui moduli di espansione tasti. Tuttavia, è necessaria un'immagine per il telefono e un'immagine per il modulo di espansione.

Il telefono analizza il colore dello sfondo e modifica il colore dei caratteri e delle icone in modo che siano leggibili. Se lo sfondo è scuro, i caratteri e le icone del telefono diventano bianche. Se lo sfondo è chiaro, ii caratteri e le icone del telefono vengono visualizzate in nero.

È consigliabile scegliere un'immagine semplice, ad esempio uno sfondo tinta unita o un motivo tinta unita. Evitare immagini ad alto contrasto.

È possibile aggiungere lo sfondo personalizzato in uno dei due seguenti modi:

- Utilizzando il file Elenco
- Utilizzando un profilo telefono comune

Se si desidera che l'utente sia in grado di selezionare l'immagine da diversi sfondi disponibili sul telefono, modificare il file Elenco. Invece se si desidera inviare l'immagine al telefono, creare o modificare un profilo telefono comune.

Indipendentemente dal metodo seguito, tenere presente quanto segue:

- Le immagini devono essere in formato PNG e l'immagine di dimensioni reali non deve superare le seguenti dimensioni:
  - Immagine in miniatura: 139 pixel (larghezza) X 109 pixel (altezza)
  - Telefono IP Cisco serie 8800: 800 pixel x 480 pixel
  - Modulo di espansione tasti del telefono IP Cisco 8851 e 8861 con schermo LCD doppio: 320 x 480 pixel
  - Modulo di espansione tasti del telefono IP Cisco 8865 con schermo LCD doppio: 320 x 480 pixel
  - Modulo di espansione tasti del telefono IP Cisco 8800 con schermo LCD singolo: 272 x 480 pixel
- Caricare le immagini, le miniature e i file Elenco sul server TFTP. La directory è:
  - Telefono IP Cisco serie 8800: Desktops/800x480x24
  - Modulo di espansione tasti del telefono IP Cisco 8851 e 8861 con schermo LCD doppio: Desktops/320x480x24
  - Modulo di espansione tasti del telefono IP Cisco 8865 con schermo LCD doppio: Desktops/320x480x24
  - Modulo di espansione tasti del telefono IP Cisco 8800 con schermo LCD singolo: Desktops/272x480x24

  Al termine del caricamento, riavviare il server TFTP.
- Se non si desidera che l'utente selezioni lo sfondo, disabilitare **Abilita l'accesso dell'utente finale all'impostazione dell'immagine di sfondo telefono**. Salvare e applicare il profilo del telefono. Riavviare il telefono in modo che le modifiche vengono applicate.

Nota È possibile applicare le immagini di sfondo del telefono in blocco con il **Profilo telefono comune**. Tuttavia, per la configurazione in blocco è necessario disabilitare **Abilita l'accesso dell'utente finale all'impostazione dell'immagine di sfondo telefono**. Per ulteriori informazioni sulla configurazione in blocco delle immagini di sfondo, fare riferimento al capitolo «Configurazione del profilo telefono comune» delle Procedure consigliate per sfondi personalizzati per telefono IP Cisco serie 8800.

Per ulteriori informazioni sulla personalizzazione dello sfondo, consultare la seguente documentazione:

- Procedure consigliate per sfondi personalizzati per telefono IP Cisco serie 8800).
- "Squilli e sfondi personalizzati" della Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager per Cisco Unified Communications Manager 12.0(1) o versioni successive.
- Capitolo «Impostazioni» della *Guida per l'utente del telefono IP Cisco serie 8800*.

Impostazione del codec wideband

Il codec G.722 è abilitato per impostazione predefinita sul telefono IP Cisco. Se Cisco Unified Communications Manager è configurato per l'uso del codec G.722 e se l'endpoint remoto supporta tale codec, la chiamata si connette tramite il codec G.722 invece che tramite il codec G.711.

Questa situazione si verifica indipendentemente dall'abilitazione da parte dell'utente di una cuffia o di un ricevitore Wideband. Tuttavia, se il ricevitore o la cuffia sono abilitati, l'utente può notare una maggiore sensibilità dell'audio durante la chiamata. Tale maggiore sensibilità comporta non solo un miglioramento della chiarezza dell'audio, ma anche un aumento dei rumori di sottofondo (come il fruscio di fogli di carta o delle conversazioni nelle vicinanze) avvertiti dall'endpoint remoto. Anche senza un ricevitore o una cuffia Wideband, alcuni utenti trovano la maggiore sensibilità offerta dal codec G.722 di disturbo. Altri utenti, invece, preferiscono utilizzare il codec G.722 e usufruire della maggiore sensibilità offerta.

Il parametro di servizio Annuncia codec G.722 iSAC influisce sulla disponibilità del supporto wideband per tutti i dispositivi registrati nel server Cisco Unified Communications Manager o per un telefono specifico, in base alla finestra di Cisco Unified Communications Manager Administration in cui è configurato tale parametro.

Procedura

Passaggio 1 Per configurare il supporto wideband per tutti i dispositivi:

a) Da Cisco Unified Communications Manager Administration, selezionare **Sistema** > **Parametri aziendali**.
b) Impostare il campo Annuncia codec G.722 iSAC.

Il valore predefinito di questo parametro aziendale è **Vero** e pertanto tutti i modelli dei telefoni IP Cisco registrati su questo server Cisco Unified Communications Manager annunciano il codec G.722 in Cisco Unified Communications Manager. Se ciascun endpoint nella chiamata tentata supporta il codec G.722 nella serie di funzionalità, Cisco Unified Communications Manager sceglie tale codec per la chiamata qualora possibile.

Passaggio 2 Per configurare il supporto wideband per un dispositivo specifico:

a) Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.
b) Impostare il parametro Annuncia codec G.722 e iSAC nell'area Configurazione specifica del prodotto.

   Il valore predefinito di questo parametro specifico del prodotto è impostato sull'uso del valore specificato dal parametro aziendale. Se si desidera sovrascrivere questa impostazione sui singoli telefoni, selezionare **Abilitato** o **Disabilitato**.

Impostazione del display di inattività

È possibile specificare un display di inattività (solo testo; la dimensione del file di testo non deve superare 1 MB) sul telefono. Il display di inattività è un servizio XML richiamato dal telefono quando rimane inattivo (non in uso) e quando non viene aperto nessun menu delle funzioni per un determinato intervallo di tempo.

Per istruzioni dettagliate sulla creazione e la visualizzazione del display di inattività, consultare *Creazione della grafica di inattività URL sul telefono IP Cisco* disponibile all'URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

Inoltre, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso per le informazioni seguenti:

- Per specificare l'URL del servizio XML del display di inattività:
  - Per un telefono singolo: campo Inattivo nella finestra Configurazione telefono in Cisco Unified Communications Manager Administration.
  - Per più telefoni contemporaneamente: campo Inattività URL nella finestra Configurazione parametri Enterprise o campo Inattivo nello strumento BAT (Bulk Administration Tool).
- Per specificare l'intervallo di tempo in cui il telefono non viene utilizzato prima che venga richiamato il servizio XML del display di inattività:
  - Per un telefono singolo: campo Timer inattività nella finestra Configurazione telefono in Cisco Unified Communications Manager Administration.
  - Per più telefoni contemporaneamente: campo Tempo inattività URL nella finestra Configurazione parametri Enterprise o campo Timer inattività nello strumento BAT (Bulk Administration Tool).

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Nel campo Inattivo, immettere l'URL del servizio XML del display di inattività.

Passaggio 3 Nel campo Timer inattività, immettere l'intervallo di tempo che deve trascorrere prima che venga visualizzato il servizio XML del display di inattività.

Passaggio 4 Selezionare **Salva**.

Personalizzazione del segnale di linea

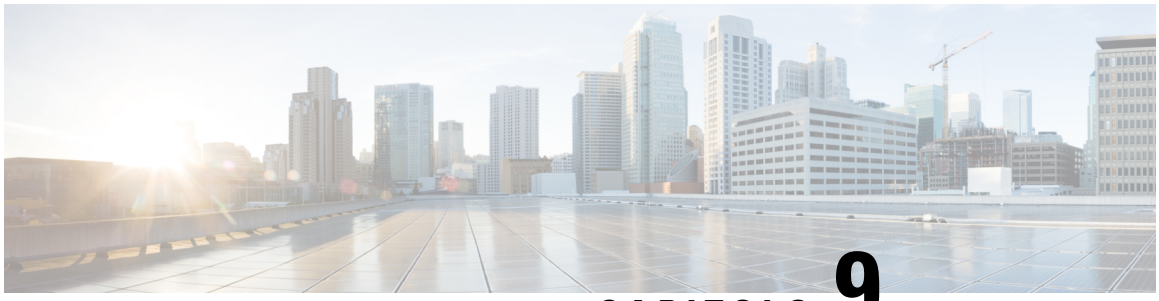
È possibile impostare i telefoni in modo che gli utenti sentano segnali di linea diversi per le chiamate interne ed esterne. A seconda delle esigenze, è possibile scegliere tra tre opzioni di segnale di linea:

- Impostazione predefinita: un segnale di linea diverso per le chiamate interne ed esterne.
- Interno: il segnale di linea interno viene utilizzato per tutte le chiamate.
- Esterno: il segnale di linea esterno viene utilizzato per tutte le chiamate.

Usa sempre segnale di linea è un campo obbligatorio in Cisco Unified Communications Manager.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Sistema** > **Parametri servizio**.
Passaggio 2	Selezionare il servizio appropriato.
Passaggio 3	Selezionare **Cisco CallManager** come servizio.
Passaggio 4	Scorrere fino al riquadro Parametri a livello di cluster.
Passaggio 5	Impostare **Usa sempre segnale di linea** su una delle seguenti opzioni: • Esterno • Interno • Impostazione predefinita
Passaggio 6	Selezionare **Salva**.
Passaggio 7	Riavviare i telefoni.



CAPITOLO 9

Configurazione e funzioni del telefono

Panoramica della configurazione e delle funzioni del telefono

Dopo aver installato i telefoni IP Cisco nella rete, configurato le relative impostazioni di rete e aver aggiunto tali telefoni a Cisco Unified Communications Manager, è necessario utilizzare l'applicazione Cisco Unified Communications Manager Administration per configurare le funzioni del telefono, modificare facoltativamente i modelli del telefono, impostare i servizi e assegnare gli utenti.

È possibile modificare le impostazioni aggiuntive del telefono IP Cisco da Cisco Unified Communications Manager Administration. Utilizzare questa applicazione basata sul Web per impostare i criteri di registrazione del telefono e le aree di ricerca chiamate, per configurare servizi e rubriche aziendali e per modificare i modelli dei pulsanti del telefono, tra le altre attività.

L'aggiunta di funzionalità ai tasti linea è limitata dal numero dei tasti linea disponibili. Non è possibile aggiungere altre funzioni al numero di tasti linea sul telefono.

Supporto utente per il telefono IP Cisco

In genere l'amministratore del sistema è la fonte principale delle informazioni date agli utenti dei telefoni IP Cisco nella propria rete o all'interno della società. È importante fornire informazioni aggiornate e complete agli utenti finali.

Per utilizzare correttamente alcune delle funzioni del telefono IP Cisco (tra cui Servizi e le opzioni del sistema di messaggistica vocale), è necessario che gli utenti ricevano informazioni da parte dell'amministratore o del team di rete o che siano in grado di contattare l'amministratore per richiedere assistenza. Assicurarsi di fornire agli utenti i contatti dei membri del team e le istruzioni da seguire per richiedere un intervento di supporto.

Si consiglia di creare una pagina Web sul sito del supporto interno in cui riportare tutte le informazioni importanti sui telefoni IP Cisco.

Prendere in considerazione l'inclusione dei seguenti tipi di informazioni sul sito:

- Guide per l'utente per tutti i modelli di telefoni IP Cisco supportati
- Informazioni sull'accesso al portale Self Care di Cisco Unified Communications
- Elenco delle funzioni supportate
- Guida per l'utente o guida di riferimento rapido sul sistema di posta vocale

Funzioni del telefono

Dopo aver aggiunto i telefoni IP Cisco a Cisco Unified Communications Manager, è possibile aggiungere funzionalità ai telefoni. La tabella che segue contiene un elenco di funzioni telefoniche supportate, molte delle quali sono configurabili tramite Cisco Unified Communications Manager Administration.

Per informazioni sull'uso della maggior parte di queste funzioni sul telefono, vedere la *Guida per l'utente del telefono IP Cisco serie 8800*. Consultare Tasti funzione e softkey, a pagina 142 per un elenco delle funzioni configurabili come pulsanti programmabili e softkey e tasti funzione dedicati.

Nota Cisco Unified Communications Manager Administration fornisce inoltre diversi parametri di servizio utilizzabili per configurare diverse funzioni di telefonia. Per ulteriori informazioni sull'accesso e la configurazione dei parametri di servizio, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Per ulteriori informazioni sulle funzioni di un servizio, selezionare il nome del parametro o il pulsante della **guida con il punto interrogativo (?)** nella finestra Configurazione specifica del prodotto.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Composizione abbreviata	Consente agli utenti di comporre rapidamente un numero di telefono immettendo un codice indice assegnato (da 1 a 199) sulla tastiera del telefono. **Nota** È possibile utilizzare la composizione abbreviata con il ricevitore agganciato o sganciato. Gli utenti assegnano codici indice dal portale Self Care.

Funzione	Descrizione e ulteriori informazioni
Allarme chiam in entrata operativo	Fornisce diverse opzioni per controllare gli allarmi delle chiamate in entrata. È possibile abilitare o disabilitare l'allarme di chiamata. È inoltre possibile attivare o disattivare la visualizzazione dell'ID del chiamante. Vedere Allarme chiam in entrata operativo, Configurazione specifica del prodotto, a pagina 146.
Supporto crittografia AES 256 per i telefoni	Migliora la sicurezza tramite il supporto di TLS 1.2 e nuovi codici. Per ulteriori informazioni, consultare Funzioni di protezione supportate, a pagina 88.
Formula di apertura agente	Consente di creare e aggiornare una formula di saluto pre-registrata che viene riprodotta all'inizio della chiamata di un cliente, prima che l'agente avvii la conversazione con il chiamante. L'agente può preregistrare una o più formule di apertura a seconda delle esigenze. Consultare Abilitazione della funzione Formula di apertura agente, a pagina 176.
Risposta per assente	Consente agli utenti di rispondere a una chiamata su una linea qualsiasi nel loro gruppo di risposta per assente, indipendentemente dalla modalità di indirizzamento della chiamata al telefono. Consultare la sezione relativa alla risposta per assente nella documentazione della versione di Cisco Unified Communications Manager in uso.
Regole di composizione applicazione	Convertono i numeri dei contatti del cellulare condivisi in numeri componibili sulla rete. Consultare Regole di composizione applicazione, a pagina 80.
Parcheggio chiamata indirizzato assistito	Consente agli utenti di parcheggiare una chiamata premendo solo un pulsante mediante la funzione di parcheggio diretto. Gli amministratori devono configurare un pulsante Parcheggio chiamata indirizzato assistito con indicatore di stato. Quando gli utenti premono un pulsante Parcheggio chiamata indirizzato assistito con indicatore di stato inattivo per una chiamata attiva, quest'ultima viene parcheggiata nello slot di parcheggio diretto associato al pulsante Parcheggio chiamata indirizzato assistito. Consultare la sezione relativa al parcheggio chiamata indirizzato assistito nella documentazione della versione di Cisco Unified Communications Manager in uso.
Indicatore acustico di messaggio in attesa (AMWI)	Un segnale acustico intermittente dal ricevitore, dalle cuffia o dall'altoparlante indica che sono presenti uno o più messaggi vocali sulla linea dell'utente. **Nota** Il segnale acustico intermittente è specifico della linea. Viene riprodotto solo quando si utilizza la linea in cui si trovano i messaggi in attesa.
Risposta automatica	Collega automaticamente le chiamate in arrivo dopo uno o due squilli. La risposta automatica funziona con le cuffie o con l'altoparlante. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Sincronizzazione porta automatica	Sincronizza le porte del telefono sulla velocità inferiore per eliminare la perdita di pacchetti. Vedere Sincronizzazione porta automatica, Configurazione specifica del prodotto, a pagina 146.
Risposta per assente automatica	Consente a un utente di utilizzare la funzioni di risposta per assente one-touch per questa funzione. Consultare la sezione relativa alla risposta per assente nella documentazione della versione di Cisco Unified Communications Manager in uso.
Inclusione	Consente a un utente di partecipare a una chiamata stabilendo una conferenza a tre tramite il ponte conferenza del telefono di destinazione. Consultare «InclusConf» in questa tabella.
Blocca esterno per trasferimento esterno	Impedisce agli utenti di trasferire una chiamata esterna a un altro numero esterno. Consultare la sezione relativa al trasferimento di chiamata esterno nella documentazione della versione di Cisco Unified Communications Manager in uso.
Multiconnessione Bluetooth	Consente all'utente di associare più dispositivi al telefono. L'utente può quindi connettere contemporaneamente tramite Bluetooth un dispositivo mobile e una cuffia Bluetooth. Il telefono IP Cisco 8851NR non supporta il Bluetooth.
Indicatore di stato	Consente a un utente di monitorare lo stato di chiamata di un numero di rubrica associato al tasto di chiamata rapida sul telefono. Per informazioni sulla presenza, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Risposta per assente con indicatore di stato	Fornisce miglioramenti alla chiamata rapida con indicatore di stato. Consente di configurare un numero di rubrica (DN) che l'utente può monitorare per le chiamate in arrivo. Quando il DN riceve una chiamata in arrivo, il sistema avvisa l'utente che può rispondere. Per informazioni sulla risposta per assente, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Prenotazione di chiamata	Fornisce agli utenti un avviso audio e visivo sul telefono quando una parte occupata o non disponibile diventa disponibile. Consultare la sezione relativa alla prenotazione di chiamata nella documentazione della versione di Cisco Unified Communications Manager in uso.
Limitazioni di visualizzazione chiamata	Determina le informazioni visualizzate sulle linee collegate o in chiamata, in base alle parti coinvolte nella chiamata. Consultare le sezioni relative ai piani di indirizzamento e alle restrizioni di visualizzazione delle chiamate nella documentazione della versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Inoltro di chiamata	Consente agli utenti di reindirizzare le chiamate in arrivo a un altro numero. Le opzioni di Deviazione chiamate comprendono Deviazione di tutte le chiamate, Devia chiamata se occupato, Devia chiamata senza risposta e Devia chiamata con nessuna copertura. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso e in Personalizzazione della visualizzazione del portale Self Care, a pagina 84.
Interruzione loop Deviazione di tutte le chiamate	Rileva e impedisce i loop di Deviazione di tutte le chiamate. Quando viene rilevato un loop di Deviazione di tutte le chiamate, la configurazione Deviazione di tutte le chiamate viene ignorata e la chiamata continua a squillare.
Divieto loop Deviazione di tutte le chiamate	Rileva e impedisce i loop di Deviazione di tutte le chiamate. Quando viene rilevato un loop di Deviazione di tutte le chiamate, la configurazione Deviazione di tutte le chiamate viene ignorata e la chiamata continua a squillare.
Visualizzazione configurabile di Deviazione chiamate	Impedisce a un utente di configurare una destinazione per Deviazione di tutte le chiamate direttamente sul telefono che crea il loop di Deviazione di tutte le chiamate o una catena di Deviazione di tutte le chiamate con più hop di quanto consentito dal parametro del servizio Numero hop massimo deviazione. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Ignora destinazione di inoltro di chiamata	Consente di ignorare l'Inoltro di tutte le chiamate (CFA) nei casi in cui la destinazione CFA effettua una chiamata verso l'iniziatore di CFA. Questa funzione consente alla destinazione CFA di raggiungere l'iniziatore di CFA per le chiamate importanti. La funzione opera sia che il numero di telefono di destinazione di CFA sia interno o esterno. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Notifica di inoltro di chiamata	Consente di configurare le informazioni visualizzate dall'utente alla ricezione di una chiamata inoltrata. Consultare Impostazione delle notifiche di deviazione chiamate, a pagina 178.
Cronologia chiamate per la linea condivisa	Consente di visualizzare l'attività della linea condivisa nella cronologia delle chiamate del telefono. Questa funzione: • Registra le chiamate perse per una linea condivisa. • Registra tutte le chiamate a cui si è risposto e le chiamate effettuate per una linea condivisa.

Funzione	Descrizione e ulteriori informazioni
Parcheggio chiamata	Consente agli utenti di parcheggiare (archiviare temporaneamente) una chiamata e quindi di recuperarla con un altro telefono nel sistema Cisco Unified Communications Manager. È possibile configurare il campo **Dedica una linea al parcheggio di chiamata** nel riquadro**Layout configurazione specifica del prodotto** per parcheggiare la chiamata sulla linea di origine o su una linea diversa. Se il campo è abilitato, la chiamata parcheggiata rimane sulla linea del cliente e può utilizzare il softkey **Riprendi** per rispondere alla chiamata. L'utente visualizza il numero di interno della chiamata parcheggiata sul display del telefono. Se il campo è disabilitato, la chiamata parcheggiata viene trasferita alla linea di parcheggio di chiamata. La linea dell'utente torna in stato inattivo e vede l'interno del parcheggio chiamata in una finestra popup. L'utente compone l'interno per rispondere alla chiamata. Per informazioni sul parcheggio delle chiamate, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Risposta per assente	Consente agli utenti di reindirizzare al proprio telefono una chiamata in arrivo su un altro telefono nel loro gruppo di risposta. È possibile configurare un avviso audio e visivo per la linea principale del telefono. Questo avviso notifica agli utenti la presenza di una chiamata in arrivo nel loro gruppo di risposta. Per informazioni sulla risposta per assente, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Registrazione chiamate	Consente a un supervisore di registrare una chiamata attiva. L'utente può udire un tono di avviso di registrazione durante la chiamata che viene registrata. Quando una chiamata è protetta, lo stato di protezione della chiamata viene visualizzato con un'icona di lucchetto sui telefoni IP Cisco. Anche le parti collegate potrebbero udire un tono di avviso che indica che la chiamata è protetta e registrata. **Nota** Durante il monitoraggio o la registrazione di una chiamata attiva, l'utente può ricevere o effettuare delle chiamate con interfono; tuttavia, se l'utente effettua una chiamata con interfono, la chiamata attiva viene messa in attesa, causando così l'interruzione della sessione di registrazione e la sospensione della sessione di monitoraggio. Per riprendere la sessione di monitoraggio, la parte di cui viene monitorata la chiamata deve riprendere la chiamata. Consultare la sezione relativa al monitoraggio e alla registrazione nella documentazione della versione di Cisco Unified Communications Manager in uso.
Avviso di chiamata	Indica (e consente agli utenti di rispondere a) una chiamata in arrivo che squilla durante un'altra chiamata. Le informazioni sulla chiamata in arrivo vengono visualizzate sul display del telefono. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Suoneria di avviso di chiamata	Fornisce agli utenti dell'avviso di chiamata la possibilità di scegliere una suoneria invece del segnale acustico standard. Le opzioni sono Squillo e Uno squillo. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
ID chiamante	L'identificazione del chiamante, ad esempio il numero di telefono, il nome o altro testo descrittivo, viene visualizzata sul display del telefono. Consultare le sezioni relative ai piani di indirizzamento e al numero di rubrica nella documentazione della versione di Cisco Unified Communications Manager in uso.
Blocco ID chiamante	Consente all'utente di bloccare il proprio numero di telefono o indirizzo e-mail dai telefoni con identificazione chiamante attivata. Consultare la sezione relativa ai piani di routing e al numero di rubrica nella documentazione della versione di Cisco Unified Communications Manager in uso.
Normalizzazione parte chiamante	La normalizzazione della parte chiamante presenta all'utente le chiamate con un numero di telefono selezionabile. Eventuali codici di escape vengono aggiunti al numero in modo che l'utente possa di nuovo collegarsi al chiamante con facilità. Il numero componibile viene salvato nella cronologia delle chiamate e può essere salvato nella rubrica personale.
CAST per SIP	Stabilisce la comunicazione tra Cisco Unified Video Advantage (CUVA) e i telefoni IP Cisco per supportare il video sul PC anche se il telefono IP non dispone di funzionalità video.
InclusConf	Consente a un utente di collegarsi a una chiamata non privata su una linea telefonica condivisa. InclusConf aggiunge un utente a una chiamata e la converte in conferenza, consentendo all'utente e alle altre parti di accedere alle funzioni tipiche delle conferenze. La conferenza viene creata tramite la funzione del ponte conferenza di Cisco Unified Communications Manager. Per il corretto funzionamento di InclusConf, è necessario abilitare sia il softkey che la funzione del ponte conferenza. Nella versione del firmware 10.2(2) e versioni successive, è possibile accedere alla funzione InclusConf tramite la softkey Includi. Per ulteriori informazioni, consultare il capitolo "Inclusione" della Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager.
Ricarica dispositivo mobile	Consente all'utente di ricaricare un dispositivo mobile collegandolo alla porta USB del telefono IP Cisco. Consultare la *Guida per l'utente del telefono IP Cisco serie 8800*.
Cisco Extension Mobility	Consente agli utenti di accedere all configurazione del telefono IP Cisco, come identificativi di linea, servizi e chiamate rapide, da un telefono IP Cisco condiviso. Cisco Extension Mobility è utile se gli utenti lavorano da ubicazioni diverse nell'azienda o se condividono uno spazio di lavoro con i colleghi.

Funzione	Descrizione e ulteriori informazioni
Extension Mobility nel cluster (EMCC) Cisco	Consente a un utente configurato in un cluster di accedere a un telefono IP Cisco in un altro cluster. Gli utenti di un cluster principale accedono al telefono IP Cisco in un visiting cluster. **Nota** Configurare Cisco Extension Mobility sui telefoni IP Cisco prima di configurare EMCC.
Cisco IP Manager Assistant (IPMA)	Fornisce funzioni di instradamento della chiamata e altre funzioni che consentono ai direttori e agli assistenti di gestire le chiamate in modo più efficace. Consultare Impostazione di Cisco IP Manager Assistant, a pagina 193.
Cisco IP Phone 8800, Modulo di espansione tasti Modulo di espansione tasti di Cisco IP Phone 8851/8861 Cisco IP Phone 8865, Modulo di espansione tasti	Fornisce tasti aggiuntivi tramite l'aggiunta di un modulo di espansione al telefono. Per ulteriori informazioni, consultare *Guida agli accessori del telefono IP Cisco serie 7800 e 8800 per Cisco Unified Communications Manager*.
Telefono IP Cisco 8811Supporto	Fornisce il supporto per Telefono IP Cisco 8811.
Supporto per il telefono IP Cisco 8851NR	Fornisce supporto per il telefono IP Cisco 8851NR.
Negoziazione versione Cisco Unified Communications Manager Express (Unified CME)	Cisco Unified Communications Manager Express utilizza un tag speciale nelle informazioni inviate al telefono per l'identificazione. Questo tag consente al telefono di fornire all'utente dei servizi supportati dallo switch. Consultare: • *Guida all'amministrazione del sistema Cisco Unified Communications Manager Express.* • Interazione con Cisco Unified Communications Manager Express, a pagina 23
Cisco Unified Video Advantage (CUVA)	Consente agli utenti di effettuare videochiamate con un telefono IP Cisco, un personal computer e una videocamera. **Nota** Configurare il parametro Funzionalità video nella sezione Layout configurazione specifica del prodotto in Configurazione telefono. Consultare la documentazione di Cisco Unified Video Advantage.
Cisco WebDialer	Consente agli utenti di effettuare chiamate dal Web e dalle applicazioni desktop.
Suoneria classica	Supporta delle suonerie integrate nel firmware del telefono o scaricate da Cisco Unified Communications Manager. Le suonerie disponibili sono condivise dagli altri telefoni IP Cisco. Consultare Suonerie personalizzate del telefono, a pagina 117.

Funzione	Descrizione e ulteriori informazioni
Conferenza	Consente a un utente di parlare contemporaneamente con più parti chiamando ciascun partecipante singolarmente. Le funzioni di Conferenza comprendono Conferenza e ConferAutom. Consente a un partecipante a una conferenza standard (ad hoc) di aggiungere o rimuovere partecipanti e consente inoltre ai partecipanti alla conferenza di partecipare insieme a due conferenze standard sulla stessa linea. Il parametro del servizio Conferenza adhoc avanzata, disabilitato per impostazione predefinita in Cisco Unified Communications Manager Administration, consente di abilitare queste funzioni. **Nota** Accertarsi di informare gli utenti dell'attivazione di queste funzioni.
Energy Efficient Ethernet (EEE) configurabile per porta PC e dello switch	Fornisce un metodo per controllare le funzioni EEE sulla porta PC e sulla porta dello switch abilitando o disabilitando EEE. La funzione controlla singolarmente entrambi i tipi di porta. Il valore predefinito è Abilitato. Consultare Impostazione di Energy Efficient Ethernet per la porta PC e dello switch, a pagina 179.
Dimensione carattere configurabile	Consente agli utenti di aumentare o diminuire il numero massimo di caratteri visualizzati sul telefono IP nella Cronologia chiamate e nella Schermata chiamata attraverso la modifica della dimensione del carattere. Un carattere più piccolo aumenta il numero massimo di caratteri visualizzati, mentre un carattere più grande lo diminuisce.
Applicazioni CTI	Un punto di indirizzamento CTI (Computer Telephony Integration) può designare un dispositivo virtuale per ricevere più chiamate simultanee per il reindirizzamento controllato dall'applicazione.
Rifiuta Tutte	Consente all'utente di trasferire una chiamata in arrivo, connessa o in attesa direttamente a un sistema di voice messagging. Quando una chiamata viene rifiutata, la linea diventa disponibile per effettuare o ricevere nuove chiamate. Consultare la sezione relativa alla deviazione immediata nella documentazione della versione di Cisco Unified Communications Manager in uso.
Registrazione richiesta dal dispositivo	Consente agli utenti finali di registrare le loro chiamate telefoniche tramite una softkey. Inoltre, gli amministratori possono continuare a registrare le chiamate tramite l'interfaccia utente CTI. Consultare la sezione relativa al monitoraggio e alla registrazione nella documentazione della versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Parcheggio chiamata indirizzato	Consente all'utente di trasferire una chiamata attiva a un numero di parcheggio chiamata indirizzato disponibile composto dall'utente normalmente o tramite le chiamate rapide. Il pulsante Indicatore di stato parcheggio chiamata indica se un numero di parcheggio chiamata indirizzato è occupato e fornisce accesso tramite chiamata rapida al numero di parcheggio chiamata indirizzato. **Nota** Se si implementa il Parcheggio chiamata indirizzato, non configurare il softkey Parcheggio, per evitare così agli utenti di confondere le due funzioni di parcheggio chiamata. Per informazioni sul parcheggio delle chiamate, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Visualizzazione delle icone relative al livello di carica della batteria e alla potenza del segnale	Visualizza sul telefono IP il livello di carica della batteria e la potenza del segnale di un cellulare quando quest'ultimo è connesso al telefono tramite Bluetooth. Il telefono IP Cisco 8851NR non supporta il Bluetooth.
Suoneria distintiva	Gli utenti possono personalizzare la modalità con cui il telefono indica una chiamata in arrivo e la presenza di un nuovo messaggio nella casella vocale. Per informazioni sulla risposta per assente, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Non disturbare (NoDist)	Quando l'opzione NoDist è attiva, non è possibile udire la suoneria per le chiamate oppure non sono visibili né udibili notifiche di alcun tipo. Se è abilitata, l'intestazione del telefono diventa rossa e sul telefono viene visualizzato Non disturbare. Se è configurata la·funzione·MLPP (Multilevel·Precedence·and·Preemption, Precedenza·e·prelazione·multilivello) e l'utente riceve una chiamata con precedenza, il telefono squilla con una suoneria speciale. Vedere Impostazione dell'opzione Non disturbare, a pagina 175.
Abilitazione/Disabilita JAL/TAL	Consente all'amministratore di controllare le funzioni JAL (Join Across Lines, Collega le linee) e TAL (Direct Transfer Across Lines, Trasferisci sulle linee). Vedere Criterio Collega e Trasferimento diretto, Configurazione specifica del prodotto, a pagina 146.
EnergyWise	Consente di mettere in stato di sospensione (spegnere) un telefono IP e di riattivarlo (accendere) in orari predeterminati, per risparmiare energia. Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 172.
Modalità linea avanzata	Abilitare la modalità linea avanzata per utilizzare come tasti linea i pulsanti che si trovano su entrambi i lati dello schermo del telefono. Vedere Impostazione di tasti di linea aggiuntivi, a pagina 204.

Funzione	Descrizione e ulteriori informazioni
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Migliora la funzione Secure Extension Mobility Cross Cluster (EMCC) mantenendo le configurazioni di rete e di protezione sul telefono di accesso. In questo modo, i criteri di protezione vengono mantenuti, la larghezza di banda di rete preservata e si evitano guasti di rete nel visiting cluster (VC).
Servizio di composizione veloce	Consente all'utente di immettere un codice di composizione veloce per effettuare una chiamata. I codici di composizione veloce possono essere assegnati ai numeri di telefono o alle voci della Rubrica personale. Consultare «Servizi» in questa tabella. Consultare Modifica del modello pulsanti del telefono per la rubrica personale o la composizione veloce, a pagina 202.
Risposta per assente di gruppo	Consente all'utente di rispondere a una chiamata in arrivo su un numero di rubrica di un altro gruppo. Per informazioni sulla risposta per assente, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Controllo propria voce in cuffia	Consente a un amministratore di impostare il livello della propria voce in una cuffia con cavo.
Ripristino attesa	Limita l'intervallo di tempo per cui è possibile tenere una chiamata in attesa prima di ripristinarla sul telefono che l'ha messa in attesa e avvisare l'utente. Il ripristino delle chiamate si distingue dalle chiamate in arrivo per l'emissione di un singolo squillo (o segnale acustico, in base all'impostazione dell'indicatore di nuova chiamata della linea). Se la chiamata non viene recuperata, questa notifica si ripete a intervalli. Nel fumetto della chiamata che attiva il Ripristino attesa viene visualizzata anche un'icona animata. È possibile configurare la priorità di attenzione alla chiamata per dare la precedenza alle chiamate ripristinate o a quelle in arrivo.
Stato di attesa	Consente ai telefoni con una linea condivisa di distinguere tra linee locali e remote che hanno messo in attesa una chiamata.
Attesa/Riprendi	Consente all'utente di spostare una chiamata connessa dallo stato Attivo allo stato In attesa. • Non è richiesta alcuna configurazione a meno che non si desideri utilizzare Musica di attesa. Consultare «Musica di attesa» in questa tabella per informazioni. • Consultare «Ripristino attesa» in questa tabella.
Download HTTP	Migliora il processo di download dei file sul telefono per l'utilizzo predefinito di HTTP. Se il download HTTP non riesce, il telefono torna a utilizzare il download TFTP.

Funzione	Descrizione e ulteriori informazioni
Gruppo di ricerca	Fornisce la condivisione del carico per le chiamate a un numero di rubrica principale. Un gruppo di ricerca contiene una serie di numeri di rubrica che possono rispondere alle chiamate in arrivo. Quando il primo numero di rubrica nel gruppo di ricerca è occupato, il sistema cerca con una sequenza predeterminata il successivo numero di rubrica disponibile nel gruppo e indirizza la chiamata a tale telefono. È possibile visualizzare **ID chiamante** (se è configurato l'ID chiamante), **Numero di telefono** e **Numero pilota del gruppo di ricerca** visualizzati nell'avviso di chiamata in arrivo per la chiamata al gruppo di ricerca. Il numero del gruppo di ricerca viene visualizzato dopo l'etichetta "Gruppo di ricerca". Consultare la sezione relativa al gruppo di ricerca e ai piani di indirizzamento nella documentazione della versione di Cisco Unified Communications Manager in uso.
Timer avviso popup chiamata in arrivo	Consente di impostare l'intervallo di tempo per cui un avviso popup (notifica) di chiamata in arrivo viene visualizzato sullo schermo del telefono. Vedere Timer avviso popup chiamata in arrivo, Configurazione specifica del prodotto, a pagina 146.
Intelligent Proximity	Consente agli utenti di associare un dispositivo mobile al telefono tramite Bluetooth e di utilizzare il telefono per effettuare e ricevere chiamate sul cellulare. Consultare Abilitazione di Intelligent Proximity, a pagina 208. I telefoni IP Cisco 8811, 8841 e 8851NR non supportano il Bluetooth o Intelligent Proximity.
Interfono	Consente agli utenti di effettuare e ricevere chiamate interne tramite i pulsanti programmabili del telefono. È possibile configurare i pulsanti di linea interfono per: • Comporre direttamente uno specifico numero di interno. • Iniziare una chiamata interna, quindi chiedere all'utente di immettere un numero di interno valido. **Nota** Se l'utente si connette allo stesso telefono ogni giorno utilizzando il profilo di Mobilità interni telefoni di Cisco, assegnare il modello dei pulsanti del telefono con le informazioni sull'interfono a questo profilo e assegnare il telefono come dispositivo di interfono predefinito per la linea dell'interfono.
Supporto per solo IPv6	Fornisce supporto per l'indirizzamento IP esteso sui telefoni IP Cisco. La configurazione IPv4 e IPv6 è consigliata e interamente supportata. Nella configurazione autonoma, alcune funzioni non sono supportate. Viene assegnato solo l'indirizzo IPv6. Consultare Configurazione delle impostazioni di rete, a pagina 59.
Buffer jitter	La funzione Buffer jitter gestisce il jitter da 10 millisecondi (ms) a 1000 ms per i flussi audio. Viene eseguita in una modalità adattiva e regola in modo dinamico la quantità di jitter.
Collega	Consente agli utenti di collegare due chiamate su una linea per creare una conferenza e rimanere nella chiamata.

Funzione	Descrizione e ulteriori informazioni
Stato linea per elenchi chiamate	Consente all'utente di visualizzare lo stato di disponibilità dello Stato linea dei numeri di linea monitorati nell'elenco della cronologia chiamate. Gli stati linea sono: • Non in linea • Disponibile • In uso • Non disturbare Consultare Abilitazione dell'indicatore di stato per elenchi chiamate, a pagina 178.
Stato linea nella rubrica aziendale	Abilita la visualizzazione dello stato di un contatto nella rubrica aziendale. • Non in linea • Disponibile • In uso • Non disturbare Consultare Abilitazione dell'indicatore di stato per elenchi chiamate, a pagina 178.
Etichetta di testo della linea	Imposta un'etichetta di testo per una linea telefonica invece del numero di rubrica. Consultare Impostazione di un'etichetta per una linea, a pagina 187.
Disconnessione dai gruppi di ricerca	Consente agli utenti di disconnettersi dal gruppo di ricerca e bloccare temporaneamente le chiamate ai loro telefoni quando non sono disponibili per rispondere. La disconnessione dai gruppi di ricerca non impedisce la ricezione sul proprio telefono di chiamate non appartenenti ai gruppi di ricerca. Consultare la sezione relativa al piano di indirizzamento nella documentazione della versione di Cisco Unified Communications Manager in uso.
Identificazione chiamate indesiderate (MCID, Malicious Call Identification)	Consente agli utenti di notificare all'amministratore di sistema eventuali chiamate sospette ricevute.
Conferenza automatica	Consente a un utente di avviare una Conferenza automatica nella quale gli altri partecipanti chiamano un numero predeterminato a un'ora pianificata.
Messaggio in attesa	Definisce i numeri di rubrica per gli indicatori on e off dei messaggi in attesa. Un sistema di messaggistica vocale connesso direttamente utilizza il numero di rubrica specificato per impostare o cancellare un'indicazione di messaggio in attesa per un determinato telefono IP Cisco. Consultare la sezione relativa ai messaggi in attesa e alla casella vocale nella documentazione della versione di Cisco Unified Communications Manager in uso.
Indicatore di messaggio in attesa	Una spia sul ricevitore che indica che sono presenti uno o più nuovi messaggi vocali per un utente. Consultare la sezione relativa ai messaggi in attesa e alla casella vocale nella documentazione della versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Volume suoneria minimo	Imposta un livello minimo per il volume della suoneria per un telefono IP.
Registrazione chiamata non risposta	Consente a un utente di specificare se le chiamate non risposte verranno registrate nella relativa rubrica per un determinato aspetto di linea. Consultare la sezione relativa al numero di rubrica nella documentazione della versione di Cisco Unified Communications Manager in uso.
Connessione mobile	Consente agli utenti di gestire le chiamate aziendali tramite un singolo numero di telefono e di rispondere alle chiamate in corso con il telefono da scrivania e con un dispositivo remoto, ad esempio un cellulare. Gli utenti possono limitare il gruppo di chiamanti in base a numero di telefono e all'ora del giorno. Consultare la sezione relativa a Cisco Unified Mobility nella documentazione della versione di Cisco Unified Communications Manager in uso.
Mobile and Remote Access Through Expressway	Consente ai lavoratori remoti di connettersi con facilità e in sicurezza alla rete aziendale senza utilizzare un tunnel client VPN (virtual private network). Vedere Mobile and Remote Access Through Expressway, a pagina 181.
Mobile Voice Access	Estende le funzionalità di connessione mobile consentendo agli utenti di accedere a un sistema di risposta vocale interattiva (IVR) per originare una chiamata da un dispositivo remoto come un telefono cellulare. Consultare la sezione relativa a Cisco Unified Mobility nella documentazione della versione di Cisco Unified Communications Manager in uso.
Monitoraggio e registrazione	Consente a un supervisore di monitorare in modalità invisibile una chiamata attiva. Il supervisore non può essere ascoltato dall'altra parte della chiamata. L'utente può udire un tono di avviso di monitoraggio durante la chiamata che viene monitorata. Quando una chiamata è protetta, lo stato di protezione della chiamata viene visualizzato con un'icona di lucchetto sui telefoni IP Cisco. Anche le parti collegate potrebbero udire un tono di avviso che indica che la chiamata è protetta e monitorata. **Nota** Quando una chiamata attiva viene monitorata o registra, l'utente può ricevere o effettuare chiamate con interfono; tuttavia, se l'utente effettua una chiamata con interfono, la chiamata attiva viene messa in attesa, causando così l'interruzione della sessione di registrazione e la sospensione della sessione di monitoraggio. Per riprendere la sessione di monitoraggio, la parte di cui viene monitorata la chiamata deve riprendere la chiamata.
Precedenza e prelazione multilivello	Consente all'utente di fare e ricevere chiamate urgenti o critiche in alcuni ambienti specializzati come uffici militari o statali. Consultare Precedenza e prelazione multilivello, a pagina 197.

Funzione	Descrizione e ulteriori informazioni
Più chiamate per aspetto linea	Ciascuna linea può supportare più chiamate. Per impostazione predefinita, il telefono supporta due chiamate attive per linea, fino a un massimo di sei chiamate attive per linea. È possibile connettere una sola chiamata alla volta. Le altre chiamate vengono automaticamente messe in attesa. Il sistema consente di configurare un massimo di chiamate/trigger di occupato non superiore a 6/6. Non sono ammesse configurazioni che superano tale limite. Consultare la sezione relativa al numero di rubrica nella documentazione della versione di Cisco Unified Communications Manager in uso.
Musica di attesa	Riproduce della musica durante l'attesa dei chiamanti.
Disattiva audio	Disattiva il microfono del ricevitore o della cuffia.
Nessun nome di avviso	Semplifica agli utenti finali l'identificazione delle chiamate trasferite tramite la visualizzazione del numero di telefono del chiamante originale. La chiamata viene visualizzata come una chiamata di avviso seguita dal numero di telefono del chiamante.
Composizione con ricevitore agganciato	Consente all'utente di comporre un numero senza sganciare il ricevitore. L'utente può quindi sollevare il ricevitore o premere Chiama.
Altra risposta per assente di gruppo	Consente a un utente di rispondere a una chiamata in arrivo su un telefono di un altro gruppo associato al gruppo dell'utente. Per informazioni sulla risposta per assente, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Messaggio display telefono per utenti di Mobilità interni telefonici	Questa funzione migliora l'interfaccia del telefono per l'utente di mobilità interni fornendo utili messaggi.
Notifica Trust List del telefono in Cisco Unified Communications Manager	Consente al telefono di inviare un avviso a Cisco Unified Communications Manager quando la Trust List (TL) viene aggiornata. Consultare Funzioni di protezione supportate, a pagina 88.
Supporto PLK per Statistiche coda	La funzione Supporto PLK per Statistiche coda consente all'utente di interrogare le statistiche della coda di chiamata sui pilot di ricerca. Le informazioni vengono visualizzate sullo schermo del telefono.
Composizione di un numero con il segno + (più)	Consente all'utente di comporre numeri E.164 preceduti dal segno più (+). Per digitare il segno +, l'utente deve tenere premuto il tasto asterisco (*) per almeno 1 secondo. Questa funzione è valida per digitare la prima cifra per le chiamate con ricevitore agganciato (compresa la modalità di modifica) o sganciato.
Negoziazione alimentazione su LLDP	Consente al telefono di negoziare l'alimentazione mediante i protocolli LLDP (Link Level Endpoint Discovery Protocol) e CDP (Cisco Discovery Protocol). Vedere Negoziazione alimentazione, Configurazione specifica del prodotto, a pagina 146.

Funzione	Descrizione e ulteriori informazioni
Composizione predittiva	Semplifica l'esecuzione di una chiamata L'elenco Recenti mostra le modifiche per visualizzare solo i numeri di telefono simili al numero composto. La composizione predittiva viene attivata quando è attivata la modalità linea avanzata. Affinché la composizione predittiva funzioni, è necessario disabilitare IU semplificata nuova chiamata.
Privacy	Impedisce agli utenti che condividono una linea di aggiungersi a una chiamata e di visualizzare informazioni sul display del loro telefono relative alla chiamata di un altro utente. Consultare la sezione relativa all'inclusione e alla privacy nella documentazione della versione di Cisco Unified Communications Manager in uso.
Private Line Automated Ringdown (PLAR)	L'amministratore di Cisco Unified Communications Manager può configurare un numero di telefono composto dal telefono IP Cisco non appena l'utente sgancia il ricevitore. Ciò può essere utile per i telefoni da cui si devono chiamare numeri di emergenza o «hotline». L'amministratore può configurare un ritardo fino a un massimo di 15 secondi. Ciò consente all'utente di effettuare una chiamata prima che per impostazione predefinita venga utilizzato per il telefono il numero della hotline. Il timer è configurabile tramite il parametro **Off Hook To First Digit Timer** in **Device** > **Device Settings** > **SIP Profile** (Timer dallo sganciamento al primo numero in Dispositivo > Impostazioni dispositivo > Profilo SIP). Per ulteriori informazioni, consultare la *Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager*.
Strumento segnalazione problemi (PRT)	Invia i registri del telefono o le segnalazioni sui problemi a un amministratore. Consultare Problem Reporting Tool (PRT), a pagina 186.
Tasti funzione programmabili	È possibile assegnare funzioni come Nuova chiamata, Prenotazione di chiamata e Inoltra tutte ai pulsanti di linea. Consultare la sezione relativa al modello dei pulsanti del telefono nella documentazione della versione di Cisco Unified Communications Manager in uso.
Quality Reporting Tool (QRT)	Consente agli utenti di inviare informazioni su chiamate problematiche premendo un pulsante. È possibile configurare lo strumento QRT per una delle due modalità utente, in base al livello di interazione utente desiderata con lo strumento QRT.
Recenti	Consente agli utenti di visualizzare le 150 chiamate singole e di gruppo più recenti. È possibile visualizzare i numeri composti di recente, le chiamate non risposte ed eliminare un record di chiamata.
Ripeti	Consente agli utenti di chiamare il numero di telefono composto per ultimo premendo un pulsante o la softkey Ripeti.

Funzione	Descrizione e ulteriori informazioni
Configurazione delle porte remota	Consente di configurare la velocità e la funzione duplex delle porte Ethernet del telefono da remoto mediante Cisco Unified Communications Manager Administration. Vengono così migliorate le prestazioni per implementazioni di grandi dimensioni con impostazioni di porta specifiche. **Nota** Se le porte sono configurate per la configurazione delle porte remota in Cisco Unified Communications Manager, non è possibile modificare i dati sul telefono. Vedere Configurazione delle porte remota, Configurazione specifica del prodotto, a pagina 146.
Reindirizza le chiamate dirette alla destinazione remota al numero aziendale	Reindirizza al numero aziendale (telefono fisso) una chiamata diretta al cellulare di un utente. Per una chiamata in arrivo alla destinazione remota (cellulare), squilla solo la destinazione, mentre il telefono fisso non squilla. Quando si risponde alla chiamata in arrivo sul cellulare, sul telefono fisso viene visualizzato il messaggio Remote In Use. Durante queste chiamate, gli utenti possono utilizzare varie funzioni del loro cellulare. Consultare la sezione relativa a Cisco Unified Mobility nella documentazione della versione di Cisco Unified Communications Manager in uso.
Rimuovi timer di richiesta "Chiamata terminata"	Migliora il tempo di risposta di Termina chiamata tramite la rimozione del messaggio `Chiamata terminata` visualizzato sullo schermo del telefono.
Impostazione suoneria	Identifica il tipo di suoneria utilizzato per una linea quando sul telefono è attiva un'altra chiamata. Per informazioni sul numero di rubrica, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso e in Suonerie personalizzate del telefono, a pagina 117.
Attesa RTCP per SIP	Assicura che le chiamate in attesa non vengano interrotte dal gateway. Il gateway controlla lo stato della porta RTCP per determinare se una chiamata è attiva o meno. Tenendo aperta la porta del telefono, il gateway non interrompe le chiamate in attesa.
Conferenza protetta	Consente ai telefoni protetti di fare chiamate in conferenza mediante un ponte conferenza protetto. Man mano che nuovi partecipanti vengono aggiunti tramite le softkey Conf, Collega, Includi o tramite Conferenza ConfAut, l'icona della chiamata protetta viene visualizzata se tutti i partecipanti utilizzano telefoni protetti. L'Elenco partecipanti conferenza visualizza il livello di protezione di ciascun partecipante alla conferenza. Gli iniziatori della conferenza possono rimuovere i partecipanti non protetti dall'Elenco partecipanti conferenza. Gli utenti che non hanno iniziato la conferenza possono aggiungere o rimuovere i partecipanti alla conferenza se è stato impostato il parametro Conferenza adhoc avanzata abilitata. Consultare la sezione relativa al ponte conferenza e alla protezione nella documentazione della versione di Cisco Unified Communications Manager in uso e in Funzioni di protezione supportate, a pagina 88.
EMCC sicuro	Migliora la funzione EMCC fornendo protezione potenziata per gli utenti che accedono al telefono da un ufficio remoto.

Funzione	Descrizione e ulteriori informazioni
Servizi	Consente di utilizzare il menu di configurazione dei servizi del telefono IP Cisco in Cisco Unified Communications Manager Administration per definire e mantenere l'elenco dei servizi telefonici che l'utente può sottoscrivere. Consultare la sezione relativa ai servizi nella documentazione della versione di Cisco Unified Communications Manager in uso.
Pulsante URL servizi	Consente agli utenti di accedere ai servizi da un pulsante programmabile invece che dal menu Servizi del telefono. Consultare la sezione relativa ai servizi nella documentazione della versione di Cisco Unified Communications Manager in uso.
Mostra ID chiamante e numero chiamante	I telefoni possono visualizzare ID e numero del chiamante per le chiamate in arrivo. La lunghezza dell'ID e del numero del chiamante visualizzati sono limitati dalle dimensioni del display LCD del telefono IP. La funzione Mostra ID chiamante e numero chiamante si applica solo all'avviso di chiamata in arrivo e non apporta nessuna modifica alle funzioni inoltro di chiamata e Gruppo di ricerca. Vedere «ID chiamante» in questa tabella.
Semplificazione dell'accesso a Extension Mobility con cuffie Cisco	Consente agli utenti di accedere a Extension Mobility con le cuffie Cisco. Se il telefono è in modalità MRA, l'utente può utilizzare la cuffia per eseguire l'accesso al telefono. Questa funzione richiede Cisco Unified Communications Manager (UCM) versione 11.5(1)SU8, 11.5(1)SU.9, 12.5(1)SU3 o versione successiva. Per ulteriori informazioni, consultare la *Guida alla configurazione delle funzionalità di Cisco Unified Communications Manager* versione 12.5(1)SU8 o versione 12.5(1) SU3 o successive.
Supporto per tablet semplificato	Consente agli utenti di tablet Android o iOS di associare il tablet al telefono tramite Bluetooth e di utilizzare il telefono per la parte audio di una chiamata sul tablet. Consultare Abilitazione di Intelligent Proximity, a pagina 208. Il telefono IP Cisco 8851NR non supporta il Bluetooth.
Chiamata rapida	Chiama un numero specificato memorizzato in precedenza.
Accesso SSH	Consente di abilitare o disabilitare l'impostazione di Accesso SSH tramite Cisco Unified Communications Manager Administration. Abilitando il server SSH il telefono può accettare le connessioni SSH. Disabilitando la funzionalità del server SSH del telefono, si blocca l'accesso SSH al telefono. Vedere Accesso SSH, Configurazione specifica del prodotto, a pagina 146.
Indirizzamento ora del giorno	Limita l'accesso a funzioni specifiche di telefonia per periodo di tempo. Consultare la sezione relativa al periodo di tempo e all'indirizzamento ora del giorno nella documentazione della versione di Cisco Unified Communications Manager in uso.

Funzione	Descrizione e ulteriori informazioni
Aggiornamento fuso orario	Aggiorna il telefono IP Cisco con modifiche relative al fuso orario. Consultare la sezione relativa alla data e all'ora nella documentazione della versione di Cisco Unified Communications Manager in uso.
Trasferisci	Consente agli utenti di reindirizzare le chiamate connesse dai loro telefoni a un altro numero.
Trasferimento - Trasferimento diretto	Trasferimento: la prima richiesta di trasferimento inizia sempre una nuova chiamata con lo stesso numero di rubrica, dopo aver messo la chiamata attiva in attesa. L'utente può trasferire direttamente le chiamate tramite la funzione Trasferisci chiamata attiva. Alcune applicazioni JTAPI/TAPI non sono compatibili con l'implementazione della funzione Collega e Trasferimento diretto sul telefono IP Cisco e potrebbe essere necessario configurare il criterio Collega e Trasferimento diretto per disabilitare le relative funzioni sulla stessa linea o su più linee. Consultare la sezione relativa al numero di rubrica nella documentazione della versione di Cisco Unified Communications Manager in uso.
TVS	Trust Verification Services (TVS) consente ai telefoni di autenticare configurazioni firmate e altri server o peer senza aumentare la dimensione del Certificate Trust List (CTL) o richiedere il download di un file CTL aggiornato sul telefono. TVS è abilitato per impostazione predefinita. Il menu Impostazioni di protezione del telefono visualizza le informazioni TVS.
UCR 2013	Il telefono IP Cisco supporta Unified Capabilities Requirements (UCR) 2013 fornendo le funzioni seguenti: • Supporto di Federal Information Processing Standard (FIPS) 140-2. • Supporto di tagging 80-bit SRTCP L'amministratore di telefoni IP dovrà impostare parametri specifici in Cisco Unified Communications Manager Administration.
Notifica linea principale non configurata	Avvisa l'utente quando la linea principale non è configurata. L'utente visualizza il messaggio `Provisioning non effettuato` sullo schermo del telefono.
Aggiornamenti dell'interfaccia utente per Elenco, Avviso e Visual Voicemail	Aumenta la dimensione della finestra dell'applicazione per ridurre al minimo le stringhe troncate.
Modalità video	Consente all'utente di selezionare la modalità di visualizzazione del video per una videoconferenza, a seconda delle modalità configurate nel sistema. Consultare la sezione relativa al video nella documentazione della versione di Cisco Unified Communications Manager in uso. Disponibile solo per i telefoni IP Cisco 8845, 8865 e 8865NR.

Funzione	Descrizione e ulteriori informazioni
Supporto video	Abilita il supporto video sul telefono. È necessario abilitare il parametro Capacità video per le videochiamate nella finestra Configurazione telefono su Cisco Unified Communications Manager. Questo parametro è abilitato per impostazione predefinita. Disponibile solo per i telefoni IP Cisco 8845, 8865 e 8865NR.
Video attraverso PC	Consente agli utenti di effettuare delle videochiamate con il telefono IP Cisco Unified, un personal computer e una videocamera esterna. Questa funzione consente inoltre agli utenti di effettuare delle videochiamate con i prodotti Cisco Jabber o Cisco Unified Video Advantage.
Visual Voicemail	Sostituisce i prompt audio della casella vocale con un'interfaccia utente grafica. Consultare la *Guida di configurazione e installazione per Visual Voicemail* all'indirizzo http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3.
Sistema di messaggistica vocale	Consente ai chiamanti di lasciare dei messaggi se non si risponde alle chiamate. Consultare la sezione relativa alla casella vocale nella documentazione della versione di Cisco Unified Communications Manager in uso e in Impostazione di Visual Voicemail, a pagina 195.
VPN	Tramite SSL, fornisce una connessione VPN (Virtual Private Network) sul telefono IP Cisco Unified quando questo si trova al di fuori di una rete attendibile o quando il traffico di rete tra il telefono e Unified Communications Manager deve passare attraverso delle reti non attendibili.
Accesso Web disabilitato per impostazione predefinita	Aumenta la protezione disabilitando l'accesso a tutti i servizi Web come HTTP. Gli utenti possono accedere ai servizi Web solo se vengono abilitati.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Tasti funzione e softkey

Nella tabella seguente vengono fornite informazioni sulle funzioni disponibili sui softkey e sui tasti funzione dedicati e su quelle che è necessario configurare come tasti funzione programmabili. «Supportato» nella tabella indica che la funzione è supportata per il softkey o il tipo di tasto corrispondente. Dei due softkey e tipi di tasti, solo i tasti funzione programmabili richiedono la configurazione nell'amministrazione del telefono IP Cisco.

Per informazioni sulla configurazione dei tasti funzione programmabili, consultare Modelli dei pulsanti del telefono, a pagina 200.

Tabella 30: Funzioni e softkey e pulsanti corrispondenti

Nome funzione	Tasto funzione dedicato	Tasto funzione programmabile	Softkey
Chiamate di avviso	Non supportato	Supportato	Non supportato

Nome funzione	Tasto funzione dedicato	Tasto funzione programmabile	Softkey
Tutte le chiamate	Non supportato	Supportato	Non supportato
Rispondi	Non supportato	Supportato	Supportato
InclusConf	Non supportato	Non supportato	Supportato
Prenotazione di chiamata	Non supportato	Supportato	Supportato
Inoltro di tutte le chiamate	Non supportato	Non supportato	Supportato
Parcheggio chiamata	Non supportato	Supportato	Supportato
Stato linea Parcheggio chiamata	Non supportato	Supportato	Non supportato
Risposta per assente (RispAss)	Non supportato	Supportato	Supportato
Stato linea Risposta per Assente	Non supportato	Supportato	Non supportato
Conferenza	Supportato	Non supportato	Supportato
Devia	Non supportato	Non supportato	Supportato
Non disturbare	Non supportato	Supportato	Supportato
Risposta per assente di gruppo (RispAltriGruppi)	Non supportato	Supportato	Supportato
Attesa	Supportato	Non supportato	Supportato
Gruppi di ricerca	Non supportato	Supportato	Non supportato
Interfono	Non supportato	Supportato	Non supportato
Identificazione telefonate indesiderate (ID_TI)	Non supportato	Supportato	Supportato
Conferenza automatica	Non supportato	Supportato	Supportato
Unisci	Non supportato	Non supportato	Supportato
Connessione mobile (Mobilità)	Non supportato	Supportato	Supportato
Disattiva audio	Supportato	Non supportato	Non supportato

Nome funzione	Tasto funzione dedicato	Tasto funzione programmabile	Softkey
Risposta per altri gruppi	Non supportato	Supportato	Supportato
Supporto PLK per Stato coda	Non supportato	Non supportato	Supportato
Privacy	Non supportato	Supportato	Non supportato
Stato coda	Non supportato	Supportato	Non supportato
Quality Reporting Tool (QRT)	Non supportato	Supportato	Supportato
Registrazione	Non supportato	Non supportato	Supportato
Ripeti	Non supportato	Supportato	Supportato
Chiamata rapida	Non supportato	Supportato	Non supportato
Stato linea Chiamata rapida	Non supportato	Supportato	Non supportato
Supporto del pulsante Attesa sulle cuffie USB	Non supportato	Non supportato	Supportato
Trasferisci	Supportato	Non supportato	Supportato

Configurazione delle funzioni del telefono

È possibile configurare i telefoni in modo da offrire un'ampia gamma di funzioni, in base alle esigenze degli utenti. È possibile applicare le funzioni a tutti i telefoni, a un gruppo di telefoni o a telefoni singoli.

Quando si configurano le funzioni, nella finestra di Cisco Unified Communications Manager Administration vengono visualizzate informazioni applicabili a tutti i telefoni e informazioni applicabili al modello del telefono. Le informazioni specifiche per il modello di telefono sono riportate nell'area Layout configurazione specifica del prodotto della finestra.

Per informazioni sui campi applicabili a tutti i modelli di telefono, consultare la documentazione di Cisco Unified Communications Manager.

Quando si imposta un campo, la finestra in cui viene impostato in è importante perché è previsto un ordine di precedenza delle finestre. L'ordine di precedenza è:

1. Telefoni singoli (precedenza più alta)
2. Gruppo di telefoni
3. Tutti i telefoni (precedenza più bassa)

Ad esempio, se si desidera che le pagine Web del telefono non siano accessibili a un gruppo specifico di utenti:

1. Abilitare l'accesso alle pagine Web del telefono per tutti gli utenti.
2. Disabilitare l'accesso alle pagine Web del telefono per ogni singolo utente o impostare un gruppo di utenti e disabilitare l'accesso alle pagine Web del telefono per il gruppo di utenti.
3. Se un utente specifico del gruppo di utenti deve accedere alle pagine Web del telefono, è possibile abilitarla per quel particolare utente.

Impostazione delle funzioni del telefono per tutti i telefoni

Procedura

Passaggio 1	Accedere a Cisco Unified Communications Manager Administration come amministratore.
Passaggio 2	Selezionare **Sistema** > **Configurazione telefono aziendale**.
Passaggio 3	Impostare i campi da modificare.
Passaggio 4	Selezionare la casella di controllo **Override Enterprise Settings** (Sovrascrivi impostazioni Enterprise) per eventuali campi modificati.
Passaggio 5	Fare clic su **Salva**.
Passaggio 6	Fare clic su **Applica configurazione**.
Passaggio 7	Riavviare i telefoni.

Nota Questa operazione avrà un impatto su tutti i telefoni dell'organizzazione.

Impostazione delle funzioni del telefono per un gruppo di telefoni

Procedura

Passaggio 1	Accedere a Cisco Unified Communications Manager Administration come amministratore.
Passaggio 2	Selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**.
Passaggio 3	Individuare il profilo.
Passaggio 4	Accedere al riquadro Layout configurazione specifica del prodotto e impostare i campi.
Passaggio 5	Selezionare la casella di controllo **Override Enterprise Settings** (Sovrascrivi impostazioni Enterprise) per eventuali campi modificati.
Passaggio 6	Fare clic su **Salva**.
Passaggio 7	Fare clic su **Applica configurazione**.
Passaggio 8	Riavviare i telefoni.

Impostazione delle funzioni del telefono per un telefono singolo

Procedura

Passaggio 1	Accedere a Cisco Unified Communications Manager Administration come amministratore.
Passaggio 2	Selezionare **Dispositivo** > **Telefono**
Passaggio 3	Individuare il telefono associato all'utente.
Passaggio 4	Accedere al riquadro Layout configurazione specifica del prodotto e impostare i campi.
Passaggio 5	Selezionare la casella di controllo **Sovrascrivi impostazioni comuni** di qualsiasi campo modificato.
Passaggio 6	Fare clic su **Salva**.
Passaggio 7	Fare clic su **Applica configurazione**.
Passaggio 8	Riavviare il telefono.

Configurazione specifica del prodotto

Nella tabella seguente vengono descritti i campi del riquadro Layout configurazione specifica del prodotto.

Tabella 31: Campi di Configurazione specifica del prodotto

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Disabilia altoparlante	Casella di controllo	Non selezionata	Consente di disabilitare la funzionalità altoparlante del telefono.
Disabilita altoparlante e cuffia	Casella di controllo	Non selezionata	Consente di disabilitare la funzionalità altoparlante e cuffia del telefono.
Disabilita ricevitore	Casella di controllo	Non selezionata	Consente di disattivare le funzionalità ricevitore del telefono.
Porta PC	Abilitato Disabilitato	Abilitato	Controlla la possibilità di utilizzare la porta PC per collegare un computer alla rete LAN.
Accesso alle impostazioni	Disabilitato Abilitato Limitato	Abilitato	Abilita, disabilita o limita l'accesso alle impostazioni locali di configurazione del telefono nell'applicazione Impostazioni. • Disabilitato: nel menu Impostazioni non sono visualizzate opzioni. • Abilitato: tutte le voci nel menu Impostazioni sono accessibili. • Limitato: è accessibile solo il menu Impostazioni del telefono.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Accesso VLAN vocale dal PC	Abilitato Disabilitato	Abilitato	Indica se il telefono consente a un dispositivo collegato alla porta PC di accedere alla VLAN voce. • Disabilitato: il PC non è in grado di inviare e ricevere dati sulla VLAN vocale o dal telefono. • Disabilitato: il PC è in grado di inviare e ricevere dati dalla VLAN vocale o dal telefono. Impostare il campo su Abilitato se sul PC è in esecuzione un'applicazione per monitorare il traffico di telefono. Potrebbe trattarsi di applicazioni per il monitoraggio e la registrazione e software di monitoraggio della rete per l'analisi dei dati raccolti.
Funzionalità video	Abilitato Disabilitato	8845, 8865 e 8865NR: abilitato 8811, 8851, 8851NR, 8861: disabilitato	Consente agli utenti di effettuare videochiamate con un telefono IP Cisco, un personal computer e una videocamera.
Accesso Web	Disabilitato Abilitato	Disabilitato	Abilita o disabilita l'accesso alle pagine Web del telefono tramite un browser web. **Attenzione** Se si abilita questo campo, è possibile mostrare informazioni riservate sul telefono.
Disabilitazione di TLS 1.0 e TLS 1.1 per accesso Web	Disabilitato Abilitato	Disabilitato	Controlla l'utilizzo di TLS 1.2 per una connessione al server Web. • Disabilitato: un telefono configurato per TLS1.0, TLS 1.1 o TLS1.2 può funzionare come server HTTPs. • Abilitato: solo un telefono configurato per TLS1.2 può funzionare come server HTTPs.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Composizione Enbloc	Disabilitato Abilitato	Disabilitato	Controlla il metodo di composizione. • Disabilitato: Cisco Unified Communications Manager attende la scadenza del timer di interdigitazione in caso di sovrapposizione del piano di numerazione o del percorso di indirizzamento. • Abilitato: l'intera stringa composta viene inviata a Cisco Unified Communications Manager una volta completata la composizione. Per evitare il timeout del timer T.302, si consiglia di abilitare la composizione Enbloc in caso di sovrapposizione del piano di numerazione o del percorso di indirizzamento. La composizione Enbloc non è supportata dai codici di autorizzazione forzata (FAC) o dai codici distintivi cliente (CMC). Se si utilizza FAC o CMC per gestire l'accesso alle chiamate e la relativa contabilità, non è possibile utilizzare questa funzione.
Giorni display non attivo	Giorni della settimana		Definisce i giorni in cui il display non si accende automaticamente all'ora specificata nel campo Ora accensione display. Scegliere i giorni dall'elenco a discesa. Per scegliere più di un giorno, selezionare tutti i giorni desiderati tenendo premuto il tasto **Ctrl**.
Ora accensione display	hh:mm		Definisce l'ora in cui il display si accende automaticamente ogni giorno (tranne nei giorni specificati nel campo Giorni display non attivo). Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per accendere automaticamente il display alle 07:00 (0700), immettere 07:00. Per accendere il display alle 14:00 (1400), immettere 14:00. Se questo campo è vuoto, il display si accende automaticamente alle 00:00.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Durata accensione display	hh:mm		Definisce l'intervallo di tempo in cui il display resta acceso dopo essersi acceso all'ora specificata nel campo Ora accensione display. Ad esempio, per mantenere il display acceso per 4 ore e 30 minuti in seguito all'accensione automatica, immettere 04:30. Se questo campo è vuoto, il telefono si spegne automaticamente alla fine della giornata (00:00). Se per il campo Ora accensione display è stato immesso il valore 00:00 e per il campo della durata di accensione del display non è stato specificato nessun valore, (o è stato immesso il valore 24:00), il display non si spegne.
Timeout display non attivo	hh:mm	01:00	Definisce l'intervallo di tempo in cui il telefono non è attivo prima dello spegnimento dello schermo. Si applica solo se il display è stato acceso da un utente (tramite la pressione di un pulsante sul telefono o il sollevamento del ricevitore) mentre era spento in base alla pianificazione impostata. Immettere in questo campo un valore nel formato ore:minuti. Ad esempio, per spegnere il display dopo 1 ora e 30 minuti di inattività del telefono in seguito all'accensione del display da parte dell'utente, immettere 01:30. Per ulteriori informazioni, consultare Impostazione del display di inattività, a pagina 120.
Accen display chiam in arriv	Disabilitato Abilitato	Abilitato	Accende il display di inattività quando è in arrivo una chiamata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Abilita Power Save Plus	Giorni della settimana		Definisce la pianificazione dei giorni in cui il telefono si spegne. Scegliere i giorni dall'elenco a discesa. Per scegliere più di un giorno, selezionare tutti i giorni desiderati tenendo premuto il tasto **Ctrl**. Se Abilita Power Save Plus è attivato, si riceverà un messaggio di avviso sui problemi di ricezione delle chiamate di emergenza (e911). **Attenzione** Infatti, mentre la modalità Power Save Plus (la "Modalità") è attiva, gli endpoint configurati per questa modalità sono disabilitati per le chiamate di emergenza e per la ricezione delle chiamate in entrata. Selezionando questa modalità, si accetta quanto segue: (i) L'utente si assume la piena responsabilità nel fornire metodi alternativi per le chiamate di emergenza e la ricezione delle chiamate mentre questa modalità è attiva; (ii) Cisco declina ogni responsabilità relativamente alla scelta dell'utente di selezionare e abilitare la modalità (l'utente è l'unico responsabile); e (iii) L'amministratore accetta di informare gli utenti sulle conseguenze dell'attivazione della modalità sulle chiamate e sulle altre funzioni. Per disabilitare Power Save Plus, è necessario deselezionare la casella di controllo Consenti sostituzioni EnergyWise. Se la casella Consenti sostituzioni EnergyWise rimane selezionata ma nel campo Abilita Power Save Plus non viene selezionato nessun giorno, la modalità Power Save Plus non viene disabilitata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Ora accensione telefono	hh:mm		Determina l'ora di accensione automatica del telefono nei giorni indicati nel campo Abilita Power Save Plus. Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per accendere automaticamente il telefono alle 07:00 (0700), immettere 07:00. Per accendere il telefono alle 14:00 (1400), immettere 14:00. Il valore predefinito è vuoto e corrisponde alle 00:00. I valori immessi nel campo Ora accensione telefono devono essere di almeno 20 minuti successivi a quelli immessi nel campo Ora spegnimento telefono. Ad esempio, se il valore immesso nel campo Ora spegnimento telefono è 07:00, il valore del campo Ora accensione telefono non deve essere precedente a 07:20.
Ora spegnimento telefono	hh:mm		Identifica l'ora in cui il telefono si spegne nei giorni selezionati nel campo Abilita Power Save Plus. Se nei campi Ora accensione telefono e Ora spegnimento telefono viene immesso lo stesso valore, il telefono non si spegne. Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per spegnere automaticamente il telefono alle 7:00 (0700), immettere 7:00. Per spegnere il telefono alle 14:00 (1400), immettere 14:00. Il valore predefinito è vuoto e corrisponde alle 00:00. I valori immessi nel campo Ora accensione telefono devono essere di almeno 20 minuti successivi a quelli immessi nel campo Ora spegnimento telefono. Ad esempio, se il valore immesso nel campo Ora spegnimento telefono è 07:00, il valore del campo Ora accensione telefono non deve essere precedente a 07:20.
Timeout inattività spegnimento telefono	Da 20 a 1440 minuti	60	Indica l'intervallo di tempo in cui il telefono resta inattivo prima di spegnersi. Il timeout si verifica nelle seguenti condizioni: • Quando la modalità Power Save Plus attivata sul telefono in base alla pianificazione viene disattivata perché l'utente preme il tasto Seleziona. • Quando il telefono viene riacceso dallo switch collegato. • Quando viene raggiunta l'ora di spegnimento del telefono ma il telefono è in uso.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Abilita avviso acustico	Casella di controllo	Non selezionata	Quando abilitato, invia al telefono l'istruzione di riprodurre un avviso acustico 10 minuti prima dell'ora specificata nel campo Ora spegnimento telefono. Questa casella di controllo viene applicata soltanto se nella casella Abilita Power Save Plus sono selezionati uno o più giorni.
Dominio EnergyWise	Fino a 127 caratteri		Identifica il dominio EnergyWise in cui si trova il telefono.
Segreto EnergyWise	Fino a 127 caratteri		Identifica la password segreta di protezione utilizzata per comunicare con gli endpoint nel dominio EnergyWise.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Consenti sostituzioni EnergyWise	Casella di controllo	Non selezionata	Determina se questa casella di controllo consente di stabilire se consentire al criterio del controller del dominio EnergyWise di inviare ai telefoni gli aggiornamenti sul livello di energia. Si applicano le condizioni seguenti: • Nel campo Abilita Power Save Plus devono essere selezionati uno o più giorni. • Le impostazioni configurate in Cisco Unified Communications Manager Administration vengono applicate alla pianificazione anche se EnergyWise invia una sostituzione. Ad esempio, presupporre che l'ora di spegnimento del telefono sia impostata sulle 22:00, che il valore specificato nel campo Ora accensione telefono sia 06:00 e che nel campo Abilita Power Save Plus siano presenti uno o più giorni selezionati. • Se EnergyWise invia al telefono il comando di spegnersi alle 20:00, questa istruzione rimane attiva (presupponendo che non vi sia alcun intervento da parte dell'utente) fino alle 06:00, ovvero fino all'ora configurata per l'accensione del telefono. • Alle 06:00, il telefono si accende e riprende la ricezione delle modifiche apportate al livello di energia dalle impostazioni di Cisco Unified Communications Manager Administration. • Per modificare nuovamente il livello di energia sul telefono, EnergyWise deve inviare un nuovo comando di modifica del livello di energia. Per disabilitare Power Save Plus, è necessario deselezionare la casella di controllo Consenti sostituzioni EnergyWise. Se la casella Consenti sostituzioni EnergyWise rimane selezionata ma nel campo Abilita Power Save Plus non viene selezionato nessun giorno, la modalità Power Save Plus non viene disabilitata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Criterio Collega e Trasferimento diretto	Abilitazione Stessa linea, Più linee Abilitazione solo Stessa linea Disabilitazione Stessa linea, Più linee	Abilitazione Stessa linea, Più linee	Controlla la possibilità di collegare e trasferire le chiamate. • Abilitazione Stessa linea, Più linee: gli utenti possono trasferire o collegare direttamente una chiamata sulla linea corrente a un'altra chiamata su un'altra linea. • Abilitazione solo Stessa linea: gli utenti possono trasferire o collegare direttamente le chiamate solo quando entrambe le chiamate sono sulla stessa linea. • Disabilitazione Stessa linea, Più linee: gli utenti non possono collegare o trasferire le chiamate sulla stessa linea. Le funzioni di collegamento e trasferimento sono disabilitate e l'utente non può trasferire o collegare una chiamata direttamente.
Estendi a porta PC	Disabilitato Abilitato	Disabilitato	Indica se il telefono inoltra alla porta di accesso i pacchetti trasmessi e ricevuti sulla porta di rete.
Tono durante registrazione	Disabilitato Abilitato	Disabilitato	Controlla la riproduzione del tono quando un utente registra una chiamata.
Volume locale tono registrazione	Numero intero da 0 a 100	100	Controlla il volume del tono di registrazione per l'utente locale.
Volume remoto tono registrazione	Numero intero da 0 a 100	50	Controlla il volume del tono di registrazione per l'utente remoto.
Durata tono registrazione	Numero intero da 1 a 3000 millisecondi		Controlla la durata del tono di registrazione.
Server di registro	Stringa di 256 caratteri al massimo		Identifica il server syslog IPv4 per l'output di debug del telefono. Il formato per l'indirizzo è: **`indirizzo:<port>@@base=<0-7>;pfs=<0-1>`**
Cisco Discovery Protocol (CDP): porta dello switch	Disabilitato Abilitato	Abilitato	Controlla Cisco Discovery Protocol sulla porta SW del telefono.
Cisco Discovery Protocol (CDP): porta del PC	Disabilitato Abilitato	Abilitato	Controlla Cisco Discovery Protocol sulla porta PC del telefono.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): porta dello switch	Disabilitato Abilitato	Abilitato	Abilita LLDP-MED sulla porta SW.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Link Layer Discovery Protocol (LLDP): porta del PC	Disabilitato Abilitato	Abilitato	Abilita LLDP sulla porta del PC.
ID dell'Asset LLDP	Stringa di 32 caratteri al massimo		Identifica l'ID dell'asset assegnato al telefono per la gestione delle scorte.
Priorità alimentazione LLDP	Sconosciuto Basso Alto Critico	Sconosciuto	Assegna una priorità di alimentazione del telefono allo switch, abilitando così lo switch per fornire adeguata energia ai telefoni.
Autenticazione 802.1x	Controllato dall'utente Abilitato Disabilitato	Controllato dall'utente	Specifica lo stato della funzione di autenticazione 802.1x. • Controllato utente: l'utente può configurare 802.1x sul telefono. • Disabilitato: l'autenticazione 802.1x non è utilizzata. • Abilitato: l'autenticazione 802.1x è utilizzata e si configura l'autenticazione per i telefoni.
Sincronizzazione porta automatica	Disabilitato Abilitato	Disabilitato	Sincronizza le porte del telefono sulla velocità inferiore per eliminare la perdita di pacchetti.
Configurazione remota porta switch	Disabilitato Abilitato	Disabilitato	Consente di configurare la velocità e la funzione duplex della porta SW del telefono da remoto. Vengono così migliorate le prestazioni per implementazioni di grandi dimensioni con impostazioni di porta specifiche. Se le porte SW sono configurate per la configurazione delle porte remota in Cisco Unified Communications Manager, non è possibile modificare i dati sul telefono.
Configurazione remota porta PC	Disabilitato Abilitato	Disabilitato	Consente di configurare la velocità e la funzione duplex della porta PC del telefono da remoto. Vengono così migliorate le prestazioni per implementazioni di grandi dimensioni con impostazioni di porta specifiche. Se le porte sono configurate per la configurazione delle porte remota in Cisco Unified Communications Manager, non è possibile modificare i dati sul telefono.
Accesso SSH	Disabilitato Abilitato	Disabilitato	Controlla l'accesso al daemon SSH tramite la porta 22. Se si lascia la porta 22 aperta, il telefono sarà vulnerabile agli attacchi DoS (Denial of Service).

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Timer avviso popup chiamata in arrivo	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Mostra l'intervallo di tempo, espresso in secondi, visualizzato nell'avviso popup. In questo intervallo di tempo vengono conteggiati i tempi di dissolvenza di apertura e chiusura della finestra. 0 indica che l'avviso per le chiamate in arrivo è disabilitato.
Impostazioni internazionali della suoneria	Impostazione predefinita Giappone	Impostazione predefinita	Consente di controllare il tipo di suoneria.
Timer di riavvio TLS	Numeri intero da 0 a 3600 secondi	3600	Controlla la possibilità di riprendere una sessione TLS senza dover ripetere l'intero processo di autenticazione TLS. Se questo campo è impostato su 0, il riavvio della sessione TLS è disabilitato.
Modalità FIPS	Disabilitato Abilitato	Disabilitato	Abilita o disabilita la modalità FIPS (Federal Information Processing Standard) sul telefono.
Registra registro chiamate da linea condivisa	Disabilitato Abilitato	Disabilitato	Specifica se registrare una chiamata su linea condivisa nel registro chiamate.
Volume suoneria minimo	0-Silenzioso 1–15	0-Silenzioso	Controlla il volume minimo della suoneria del telefono. È possibile impostare un telefono in modo da non potere disattivare la suoneria.
Peer Firmware Sharing	Disabilitato Abilitato	Abilitato	Consente al telefono di individuare altri telefoni dello stesso modello sulla subnet e condividere i file del firmware aggiornati. Se il telefono dispone di un nuovo firmware, può condividerlo con gli altri telefoni. Se uno degli altri telefoni dispone di un nuovo firmware, il telefono può scaricarlo dall'altro telefono anziché dal server TFTP. Condivisione del firmware: • Limita la congestione sui trasferimenti TFTP verso i server TFTP rimossi a livello centrale. • Elimina la necessità di controllare manualmente gli aggiornamenti del firmware. • Riduce le interruzioni dell'operatività del telefono durante gli aggiornamenti mentre è in corso la reimpostazione simultanea di più telefoni. • Consente di eseguire gli aggiornamenti del firmware negli scenari di distribuzione nelle filiali o negli uffici remoti che utilizzano collegamenti WAN con larghezza di banda limitata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Server di caricamento	Stringa di 256 caratteri al massimo		Identifica il server IPv4 alternativo utilizzato dal telefono per scaricare il firmware e gli aggiornamenti. Il formato per l'indirizzo è: **indirizzo:<port>@@base=<0-7>;pfs=<0-1>**
Server di caricamento IPv6	Stringa di 256 caratteri al massimo		Identifica il server IPv6 alternativo utilizzato dal telefono per scaricare il firmware e gli aggiornamenti. Il formato per l'indirizzo è: **[indirizzo]:<port>@@base=<0-7>;pfs=<0-1>**
Controllo UI cuffia Wideband	Disabilitato Abilitato	Abilitato	Consente all'utente di utilizzare il codec wideband per la cuffia analogica.
Cuffia Wideband	Disabilitato Abilitato	Abilitato	Abilita o disabilita l'uso di una cuffia Wideband sul telefono. Utilizzato in combinazione con la cuffia Wideband controllata dall'utente. Per ulteriori informazioni, consultare Impostazione del codec wideband, a pagina 119.
Wi-Fi	Disabilitato Abilitato	Abilitato	Abilita i telefoni IP Cisco 8861 e 8865 per connettersi alla rete Wi-Fi. I telefoni che non supportano questa funzione non visualizzano il campo.
Porta USB posteriore	Disabilitato Abilitato	8861, 8865 e 8865NR: abilitato	Controlla la possibilità di utilizzare la porta USB sul retro dei telefoni IP Cisco 8861 e 8865. I telefoni che non supportano questa funzione non visualizzano il campo.
Porta USB laterale	Disabilitato Abilitato	Abilitato	Controlla la possibilità di utilizzare la porta USB laterale dei telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR. I telefoni che non supportano questa funzione non visualizzano il campo.
Accesso alla console	Disabilitato Abilitato	Disabilitato	Specifica se la console seriale è abilitata o disabilitata.
Bluetooth	Disabilitato Abilitato	Abilitato	Abilita o disabilita l'opzione Bluetooth sul telefono. Se disabilitata, l'utente non può abilitare Bluetooth sul telefono. Supportata sui telefoni IP Cisco 8845, 8851, 8861 e 8865. I telefoni che non supportano questa funzione non visualizzano il campo.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Consenti l'importazione di contatti Bluetooth	Disabilitato Abilitato	Abilitato	Consente all'utente di importare i contatti da un dispositivo mobile connesso tramite Bluetooth. Se disabilitato, l'utente non può importare nel telefono i contatti del dispositivo mobile connesso. Supportata sui telefoni IP Cisco 8845, 8851, 8861 e 8865. I telefoni che non supportano questa funzione non visualizzano il campo.
Consenti modalità vivavoce mobile Bluetooth	Disabilitato Abilitato	Abilitato	Consente agli utenti di trarre il massimo dalle proprietà acustiche del telefono utilizzando il proprio dispositivo mobile o tablet. L'utente associa il dispositivo mobile o il tablet al telefono tramite Bluetooth. Se disabilitato, l'utente non può associare il dispositivo mobile o il tablet al telefono. In seguito all'associazione del dispositivo mobile, l'utente può quindi effettuare e ricevere sul telefono le chiamate al cellulare. Con un tablet, l'utente può indirizzare l'audio dal tablet al telefono. Gli utenti possono abbinare più dispositivi mobili, tablet e cuffie Bluetooth al telefono. Tuttavia, è possibile connettere contemporaneamente solo un dispositivo e una cuffia. I telefoni che non supportano questa funzione non visualizzano il campo.
Profili Bluetooth	Viva voce Dispositivo Human Interface	Viva voce	Indica quali profili Bluetooth sul telefono sono abilitati o disabilitati. I telefoni che non supportano questa funzione non visualizzano il campo.
Gratuitous ARP	Disabilitato Abilitato	Disabilitato	Abilita o disabilita la possibilità per il telefono di identificare gli indirizzi MAC da Gratuitous ARP. Questa funzionalità è necessaria per monitorare o registrare i flussi vocali.
Visualizza tutte le chiamate su linea principale	Disabilitato Abilitato	Disabilitato	Specifica se tutte le chiamate ricevute da questo telefono verranno visualizzate sulla linea principale oppure no. Lo scopo di questo campo è consentire all'utente finale di visualizzare tutte le chiamate su tutte le linee anziché dover selezionare una linea per visualizzare le chiamate su tale linea. In altre parole, se sono configurate più linee sul telefono, in genere ha più senso poter visualizzare tutte le chiamate su tutte le linee in un'unica vista. Se questa funzione è abilitata, vengono visualizzate tutte le chiamate sulla linea principale, ma è comunque possibile scegliere una linea specifica per filtrare la visualizzazione per mostrare solo le chiamate relative a tale linea specifica.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Server HTTPS	Abilitato per HTTP e HTTPS Solo HTTPS	Abilitato per HTTP e HTTPS	Controlla il tipo di comunicazione sul telefono. Se si seleziona solo HTTPS, la comunicazione sul telefono è più sicura.
Server di registro IPv6	Stringa di 256 caratteri al massimo		Identifica il server di registro IPv6. Il formato per l'indirizzo è: `[indirizzo]:<port>@@base=<0-7>;pfs=<0-1>`
Registro remoto	Disabilitato Abilitato	Disabilitato	Controlla la possibilità di inviare i registri al server syslog.
Profilo registro	Impostazione predefinita Preimpostato Telefonia SIP UI Rete Supporti Aggiornamento Accessorio Protezione Wi-Fi VPN EnergyWise MobileRemoteAc	Preimpostato	Specifica il profilo di registrazione predefinito. • Predefinito: livello di registrazione di debug predefinito • Preimpostato: non sovrascrive l'impostazione di registrazione di debug locale del telefono • Telefonia: vengono registrate informazioni sulle funzioni di telefonia o di chiamata • SIP: vengono registrate informazioni sulla segnalazione SIP • Interfaccia utente: vengono registrate informazioni sull'interfaccia utente del telefono • Rete: vengono registrate informazioni sulla rete • Media: vengono registrate informazioni sui media • Aggiornamento: vengono registrate informazioni sull'aggiornamento • Accessori: vengono registrate informazioni sugli accessori • Sicurezza: vengono registrate informazioni sulla sicurezza • Wi-Fi: vengono registrate informazioni sul Wi-Fi • VPN: vengono registrate informazioni sulla rete privata virtuale • Energywise: vengono registrate informazioni sul risparmio energetico • MobileRemoteAC: vengono registrate informazioni sull'accesso mobile e remoto tramite Expressway

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Annuncia codec G.722 e iSAC	Usa valore predefin. sistema Disabilitato Abilitato	Usa valore predefin. sistema	Indica se il telefono pubblicizza i codec G.722 e iSAC su Cisco Unified Communications Manager. • Usa valore predefin. sistema: rinvia all'impostazione specificata nel parametro aziendale Annuncia codec G.722. • Disabilitato: non pubblicizza il codec G.722 su Cisco Unified Communications Manager. • Abilitato: pubblicizza il codec G.722 su Cisco Unified Communications Manager. Per ulteriori informazioni, vedere la nota alla fine della tabella.
Rileva errore di connessione a Unified CM	Normale Ritardato	Normale	Determina la capacità dell'applicazione telefono di rilevare un errore di connessione a Cisco Unified Communications Manager (Unified CM), che è il primo passaggio prima di che si verifichi il failover del dispositivo in un Unified CM/SRST di backup. • Normale: il rilevamento di un failover di connessione di Unified CM si verifica alla velocità di sistema standard. Scegliere questo valore per riconoscere più rapidamente un errore di connessione di Unified CM. • Ritardato: il rilevamento di un failover di connessione a Unified CM si verifica circa quattro volte più lentamente rispetto all'impostazione Normale Selezionare questo valore se si preferisce che il failover venga leggermente ritardato per consentire di ristabilire la connessione. L'esatta differenza temporale tra il rilevamento dell'errore di connessione Normale e Ritardato dipende da numerose variabili che cambiano continuamente. Questo campo si applica solo alla connessione Ethernet cablata.
Negoziazione alimentazione	Disabilitato Abilitato	Abilitato	Consente al telefono di negoziare l'alimentazione mediante i protocolli LLDP (Link Level Endpoint Discovery Protocol) e CDP (Cisco Discovery Protocol). La funzione Negoziazione alimentazione non deve essere disabilitata quando il telefono è connesso a uno switch in grado di supportarla. Se questa funzione è disabilitata, lo switch potrebbe interrompere l'erogazione dell'alimentazione al telefono.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Fornisci segnale da pulsante di rilascio	Disabilitato Abilitato	Disabilitato	Controlla se viene riprodotto il segnale di linea quando si preme il tasto Rilascia. • Disabilitato: non viene emesso il segnale di linea. • Abilitato: viene riprodotto il segnale di linea.
Immagine di sfondo	Stringa di 64 caratteri al massimo		Specifica il file di sfondo predefinito. Se è impostato uno sfondo predefinito, l'utente non può modificare lo sfondo del telefono.
IU semplificata nuova chiamata	Disabilitato Abilitato	Disabilitato	Controlla l'interfaccia utente per la composizione con ricevitore sganciato. Se abilitato, l'utente non può selezionare un numero dall'elenco delle chiamate recenti. Se abilitato, questo campo fornisce una finestra semplificata per effettuare una chiamata. L'utente non vede la finestra popup di cronologia chiamate visualizzata quando solleva il ricevitore del telefono. La visualizzazione della finestra popup viene considerata utile, quindi IU semplificata nuova chiamata è disabilitata per impostazione predefinita.
Ripristina tutte le chiamate	Disabilitato Abilitato	Disabilitato	Specifica se il telefono ripristinerà tutte le chiamate al termine di ogni chiamata se la chiamata è su un filtro diverso da Linea principale, Tutte le chiamate o Chiamate di avviso.
Mostra cronologia chiamate solo per la linea selezionata	Disabilitato Abilitato	Disabilitato	Controlla la visualizzazione dell'elenco Recenti. • Disabilitato: l'elenco Recenti mostra la cronologia chiamate per tutte le linee. • Abilitato: l'elenco Recenti mostra la cronologia chiamate della linea selezionata.
Avviso chiamata in entrata eseguibile	Disabilitato Mostra per tutte le chiamate in entrata Mostra per le chiamate in entrata nascoste	Mostra per tutte le chiamate in entrata	Controlla il tipo di avviso di chiamata in entrata visualizzato sullo schermo del telefono. Lo scopo di questo campo è ridurre il numero di pulsanti che l'utente finale deve premere per rispondere a una chiamata. • Disabilitato: l'avviso di chiamata in entrata eseguibile è disabilitato e l'utente visualizza il tradizionale avviso pop-up di chiamata in arrivo. • Mostra per tutte le chiamate in entrata: l'avviso di chiamata in entrata eseguibile viene visualizzato per tutte le chiamate a prescindere dalle impostazioni di visibilità. • Mostra per le chiamate in entrata nascoste: l'avviso di chiamata in entrata eseguibile viene visualizzato per le chiamate non visualizzate sul telefono. Questo parametro si comporta in modo simile alla notifica popup dell'avviso chiamata in entrata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Bit DF	0 1	0	Controlla la modalità di invio dei pacchetti di rete. È possibile inviare i pacchetti in blocchi (frammenti) di dimensioni diverse. Se il Bit DF è impostato su 1 nell'intestazione del pacchetto, il payload di rete non si frammenta quando passa attraverso i dispositivi di rete come ad esempio switch e router. La rimozione della frammentazione consente di evitare delle analisi errate lato ricezione, ma comporta velocità leggermente inferiori. L'impostazione del Bit DF non si applica al traffico ICMP, VPN, VXC VPN o DHCP.
Filtro linea predefinito	Elenco dei nomi dei telefoni separati da virgole		Indica l'elenco dei telefoni presenti nel filtro predefinito. Se è il filtro di linea predefinito è configurato, gli utenti visualizzano un filtro denominato `Pianificazione quotidiana` in **Notifiche chiamata** nel menu **Impostazioni** > **Preferenze** del telefono. Questo filtro di pianificazione quotidiana viene fornito in aggiunta al filtro Tutte le chiamate preimpostato. Se il filtro di linea predefinito non è configurato, il telefono seleziona tutte le linee con provisioning. Se è configurato, il telefono seleziona le linee impostate su Cisco Unified Communications Manager se l'utente seleziona il filtro Predefinito come filtro attivo o se non è presente nessun filtro personalizzato. I filtri linea personalizzati consentono di applicare filtri alle linee ad alta priorità per ridurre gli avvisi attività. È possibile impostare la priorità di notifica delle chiamate di avviso su un sottogruppo di linee protette da un filtro di avviso. Il filtro personalizzato genera avvisi popup tradizionali o avvisi eseguibili per le chiamate in arrivo sulle linee selezionate. L'avviso verrà generato, per ciascun filtro, solo dal sottoinsieme di linee protette. Questa funzione consente agli utenti con più linee di ridurre gli avvisi filtrando e visualizzando gli avvisi provenienti solo dalle linee ad alta priorità. Gli utenti finali possono configurare da soli questa opzione. In alternativa, è possibile programmare il filtro linea predefinito e applicarlo al telefono.
Priorità stato linea avviso più basso	Disabilitato Abilitato	Disabilitato	Specifica lo stato di avviso quando si utilizzano linee condivise. • Disabilitato: se è presente un avviso di chiamata in arrivo sulla linea condivisa, l'icona di stato del LED/linea riflette lo stato dell'avviso anziché l'icona Remoto in uso. • Abilitato: se è presente un avviso di chiamata in arrivo sulla linea condivisa, l'utente vede l'icona Remoto In uso.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Visualizzazione a una colonna del modulo di espansione tasti	Disabilitato Abilitato	Disabilitato	Controlla la visualizzazione sul modulo di espansione tasti. • Disabilitato: il modulo di espansione utilizza la modalità a due colonne. • Abilitato: il modulo di espansione utilizza la modalità a una colonna. I telefoni che non supportano questa funzione non visualizzano il campo.
Energy Efficient Ethernet (EEE): porta PC	Disabilitato Abilitato	Disabilitato	Controlla l'EEE sulla porta del PC.
Energy Efficient Ethernet (EEE): porta SW	Disabilitato Abilitato	Disabilitato	Controlla l'EEE sulla porta dello switch.
Porta video iniziale			Definisce l'inizio dell'intervallo di porte per le videochiamate. I telefoni che non supportano questa funzione non visualizzano il campo.
Porta video finale			Definisce la fine dell'intervallo di porte per le videochiamate. I telefoni che non supportano questa funzione non visualizzano il campo.
Credenziali utente persistenti per l'accesso a Expressway	Disabilitato Abilitato	Disabilitato	Controlla se il telefono memorizza le credenziali di accesso degli utenti. Se disabilitato, l'utente visualizza sempre la richiesta di accesso al server Expressway per l'accesso mobile e remoto (MRA). Per semplificare l'accesso agli utenti, abilitare questo campo in modo che le credenziali di accesso a Expressway siano permanenti. L'utente deve immettere le credenziali di accesso solo la prima volta. Per gli accessi successivi, se il telefono è acceso fuori sede, le credenziali di accesso sono precompilate nella schermata di accesso. Per ulteriori informazioni, vedere la sezione Mobile and Remote Access Through Expressway, a pagina 181.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
URL di caricamento assistenza clienti	Stringa di 256 caratteri al massimo		Fornisce l'URL dello strumento segnalazione problemi (PRT, Problem Reporting Tool). In caso di distribuzione dei dispositivi con accesso mobile e remoto tramite Expressway, è necessario inoltre aggiungere l'indirizzo del server PRT all'elenco degli indirizzi autorizzati del server HTTP sul server Expressway. Per ulteriori informazioni, vedere la sezione Mobile and Remote Access Through Expressway, a pagina 181.
Amministratore Web	Disabilitato Abilitato	Disabilitato	Abilita o disabilita l'accesso dell'amministratore alle pagine Web del telefono tramite un browser Web. Per ulteriori informazioni, vedere la sezione Configurazione della pagina di amministrazione per il telefono, a pagina 109. I telefoni che non supportano questa funzione non visualizzano il campo.
Password amministrativa	Stringa di 8-127 caratteri		Definisce la password dell'amministratore quando si accede alle pagine Web del telefono come amministratore. I telefoni che non supportano questa funzione non visualizzano il campo.
Server SCEP WLAN	Stringa di 256 caratteri al massimo		Specifica il Server SCEP utilizzato dal telefono per richiedere i certificati di autenticazione WLAN. Immettere il nome host o l'indirizzo IP (utilizzando il formato di indirizzamento IP standard) del server. I telefoni che non supportano questa funzione non visualizzano il campo.
Impronta digitale CA radice WLAN (SHA256 o SHA1)	Stringa di 95 caratteri al massimo		Specifica l'impronta digitale SHA256 o SHA1 dell'Autorità di certificazione principale per la convalida durante il processo SCEP quando vengono emessi i certificati per l'autenticazione WLAN. Si consiglia di utilizzare l'impronta digitale SHA256, che può essere richiesta tramite OpenSSL (ad es. openssl x509 -in rootca.cer -noout -sha256 -fingerprint) o tramite browser Web per controllare i dettagli del certificato. Immettere il valore di 64 caratteri esadecimali per l'impronta digitale SHA256 o il valore di 40 caratteri esadecimali per l'impronta digitale SHA1 con un separatore comune (due punti, trattino, punto, spazio) o senza separatore. Se si utilizza un separatore, dovrà essere inserito in modo uniforme dopo ogni 2, 4, 8, 16 o 32 caratteri esadecimali per un'impronta digitale SHA256 o ogni 2, 4 o 8 caratteri esadecimali per un'impronta digitale SHA1. I telefoni che non supportano questa funzione non visualizzano il campo.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Tentativi di autenticazione WLAN			I telefoni che non supportano questa funzione non visualizzano il campo.
Modalità prompt profilo 1 WLAN	Disabilitato Abilitato	Disabilitato	I telefoni che non supportano questa funzione non visualizzano il campo.
Modalità linea	Modalità linea sessione Modalità linea avanzata	Modalità linea sessione	Controlla la visualizzazione della linea sul telefono. • Modalità linea sessione: i pulsanti su un lato dello schermo sono i tasti di linea. • Modalità linea avanzata: i pulsanti su entrambi i lati dello schermo del telefono sono i tasti di linea. In modalità linea avanzata, la composizione predittiva e gli avvisi di chiamata in entrata eseguibili sono abilitati per impostazione predefinita.
Suoneria configurabile dall'amministratore	Disabilitato Alba Chirp1 Chirp2	Disabilitato	Regola la suoneria e consente agli utenti di impostarla. • Quando è impostato su **`Disabilitato`**, gli utenti possono configurare la suoneria predefinita sul proprio telefono. • Per tutti gli altri valori, gli utenti non possono modificare la suoneria. La voce di menu **Suoneria** nel menu **Impostazioni** è visualizzato in grigio.
Utilizzo assistenza clienti	Stringa di 64 caratteri al massimo	Vuoto	Solo per centro TAC di Cisco.
Disabilita crittografie TLS	Consultare Disabilitazione delle crittografie TLS (Transport Layer Security), a pagina 169.	Nessuno	Disabilita la crittografia TLS selezionata. Per disabilitare più di un pacchetto di crittografia, selezionare e tenere premuto il tasto **CTRL** sulla tastiera del computer. La selezione di tutte le crittografie del telefono influisce sul servizio TLS del telefono.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Avviso Abbassa la voce	Abilitato Disabilitato	Abilitato	Consente di controllare la funzione Abbassa la voce. • Disabilitato: • Il telefono non visualizza la voce di menu **Abbassa la voce** nel menu **Impostazioni**. • Gli utenti non vedranno il messaggio sullo schermo quando parlano in alto. • Abilitato: • Gli utenti controllano la voce di menu **Abbassa la voce** nel menu **Impostazioni**. Per impostazione predefinita, questo campo è impostato su **Attiva**.
Contrassegna la chiamata come spam	Abilitato Disabilitato	Abilitato	Controlla la funzioni Contrassegna la chiamata come spam. • Disabilitato: • Il telefono non visualizza il softkey **Contrassegna come spam**. • La voce **Elenco di spam** nel menu **Impostazioni** non viene visualizzata. • Se era presente un elenco di spam, l'elenco viene cancellato e non può essere recuperato. • Abilitato: • Sul telefono viene visualizzato il softkey **Contrassegna come spam**. • Viene visualizzata la voce **Elenco di spam** nel menu **Impostazioni**.
Dedica una linea al parcheggio di chiamata	Disabilitato Abilitato	Abilitato	Controlla se una chiamata parcheggiata occupa una linea o no. Per ulteriori informazioni, consultare la documentazione di Cisco Unified Communications Manager.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione e linee guida per l'utilizzo
Visualizzazione dell'etichetta di testo della linea in ELM	Disabilitato Abilitato	Abilitato	Controlla la visualizzazione dell'etichetta della linea durante una chiamata quando è configurata la modalità linea avanzata • Abilitato • Se il nome del chiamante è configurato, visualizza il nome nella prima linea della sessione di chiamata e l'etichetta della linea locale nella seconda linea. • Se il nome del chiamante non è configurato, visualizza il numero remoto nella prima linea e l'etichetta della linea locale nella seconda linea. • Disabilitato • Se il nome del chiamante è configurato, visualizza il nome nella prima linea della sessione di chiamata e il numero nella seconda linea. • Se il nome del chiamante non è configurato, viene visualizzato **solo** il numero remoto. Questo campo è richiesto.

Nota La negoziazione del codec prevede due passaggi:

1. Il telefono pubblicizza il codec supportato per Cisco Unified Communications Manager. Non tutti gli endpoint supportano lo stesso gruppo di codec.
2. Quando Cisco Unified Communications Manager riceve l'elenco dei codec supportati da tutti i telefoni coinvolti nel tentativo di chiamata, sceglie un codec supportato più di frequente in base a diversi fattori, tra cui l'impostazione dell'abbinamento della regione.

Procedure consigliate per la configurazione delle funzioni

È possibile impostare le funzioni del telefono in base alle esigenze degli utenti. Tuttavia, per determinate situazioni e distribuzioni consigliamo impostazioni che potrebbero risultare utili.

Ambienti con elevato volume di chiamate

In un ambiente con elevato volume di chiamate, si consiglia di configurare alcune funzioni in modo specifico.

Campo	Area Amministrazione	Impostazione consigliata
Usa sempre linea principale	Informazioni dispositivo	Disattivato o Attivato Per ulteriori informazioni, consultare Campo: Usa sempre linea principale, a pagina 169.
Avviso chiamata in entrata eseguibile	Layout configurazione specifica del prodotto	Mostra per tutte le chiamate in entrata
Visualizza tutte le chiamate su linea principale	Layout configurazione specifica del prodotto	Abilitato
Ripristina tutte le chiamate	Layout configurazione specifica del prodotto	Abilitato

Ambienti con più linee

In un ambiente con più linee, si consiglia di configurare alcune funzioni in modo specifico.

Campo	Area Amministrazione	Impostazione consigliata
Usa sempre linea principale	Informazioni dispositivo	Spento Per ulteriori informazioni, consultare Campo: Usa sempre linea principale, a pagina 169.
Avviso chiamata in entrata eseguibile	Layout configurazione specifica del prodotto	Mostra per tutte le chiamate in entrata
Visualizza tutte le chiamate su linea principale	Layout configurazione specifica del prodotto	Abilitato
Ripristina tutte le chiamate	Layout configurazione specifica del prodotto	Abilitato

Ambiente in modalità linea sessione

Modalità linea avanzata è lo strumento preferito per gestire la maggior parte degli ambienti di chiamata. Tuttavia, se la modalità linea avanzata non soddisfa le proprie esigenze, è possibile utilizzare la modalità di linea sessione.

Campo	Area Amministrazione	Impostazione consigliata per modalità linea sessione
Visualizza tutte le chiamate su linea principale	Layout configurazione specifica del prodotto	Disabilitato
Ripristina tutte le chiamate	Layout configurazione specifica del prodotto	Disabilitato

Campo	Area Amministrazione	Impostazione consigliata per modalità linea sessione
Avviso chiamata in entrata eseguibile	Layout configurazione specifica del prodotto	Abilitato per impostazione predefinita (versione del firmware 11.5 (1) e successive).

Argomenti correlati

Impostazione di tasti di linea aggiuntivi, a pagina 204
Funzioni disponibili in modalità linea avanzata, a pagina 205

Campo: Usa sempre linea principale

Questo campo specifica se su un telefono IP viene scelta la linea principale quando un utente sgancia il ricevitore. Se questo parametro è impostato su Vero, quando viene sganciato il telefono, viene scelta la linea principale e diventa attiva. Anche se una chiamata squilla sulla seconda linea dell'utente, quando il telefono viene sganciato, attiva solo la prima linea attiva. Non risponde alla chiamata in entrata sulla seconda linea. In questo caso, l'utente deve scegliere la seconda linea per rispondere alla chiamata. Il valore predefinito è impostato su False.

Lo scopo del campo Usa sempre linea principale è molto simile alla combinazione di Mostra tutte le chiamate sulla linea principale e Ripristina tutte le chiamate quando sono abilitate entrambe le funzioni. Tuttavia, la differenza principale è che quando Usa sempre linea principale è abilitata, le chiamate in entrata non ricevono risposta sulla seconda linea. Nella linea principale si sente solo il segnale di linea. In determinati ambienti con elevato volume di chiamate, questa è l'esperienza utente desiderata. In genere, è consigliabile lasciare questo campo disabilitato fatta eccezione per gli ambienti con elevato volume di chiamate che richiedono questa funzione.

Disabilitazione delle crittografie TLS (Transport Layer Security)

È possibile disabilitare le crittografie TLS (Transport Layer Security) con il parametro **Disabilita crittografie TLS**. Ciò consente di personalizzare la protezione per le vulnerabilità note e allineare la rete alle norme sulla crittografia in uso.

L'impostazione predefinita è Nessuna.

Per disabilitare più di un pacchetto di crittografia, selezionare e tenere premuto il tasto **CTRL** sulla tastiera del computer. La selezione di tutte le crittografie del telefono influisce sul servizio TLS del telefono. Le opzioni disponibili sono:

- Nessuno
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Per ulteriori informazioni sulla sicurezza del telefono, vedere *White paper introduttivo sulla protezione per il telefono IP Cisco serie 7800 e 8800* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Abilitazione della cronologia chiamate per la linea condivisa

Consente di visualizzare l'attività della linea condivisa nella cronologia delle chiamate. Questa funzione:

- Registra le chiamate perse di una linea condivisa.
- Registra tutte le chiamate a cui si è risposto e tutte le chiamate effettuate di una linea condivisa.

Prima di iniziare

Disabilitare la privacy prima di abilitare la cronologia delle chiamate per la linea condivisa. In caso contrario, la cronologia delle chiamate non visualizza le chiamate a cui rispondono altri utenti.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.
Passaggio 2	Individuare il telefono da configurare.
Passaggio 3	Selezionare Registra registro chiamate nel menu a discesa Linea condivisa nell'area Configurazione specifica del prodotto.
Passaggio 4	Selezionare **Abilitato** dall'elenco a discesa.
Passaggio 5	Selezionare **Salva**.

Pianificazione della modalità Risparmio energia per il telefono IP Cisco

Per risparmiare energia e garantire una durata prolungata del display del telefono, è possibile impostare il display sulla disattivazione quando non è in uso.

In Cisco Unified Communications Manager Administration, è possibile configurare le impostazioni per lo spegnimento del display in un orario stabilito in determinati giorni e per tutto il giorno in altri giorni. Ad esempio, è possibile scegliere di spegnere il display dopo l'orario di lavoro nei giorni feriali e per tutto il giorno di sabato e domenica.

È possibile effettuare una delle azioni seguenti per accendere il display quando è spento:

- Premere un pulsante qualsiasi sul telefono.

  Il telefono esegue l'azione collegata al pulsante oltre ad accendere il display.
- Sollevare il ricevitore.

Quando si accende il display, quest'ultimo rimane acceso finché il telefono rimane inattivo per un intervallo di tempo impostato e successivamente si spegne automaticamente.

Per ulteriori informazioni, consultare Configurazione specifica del prodotto, a pagina 146

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono da impostare.

Passaggio 3 Accedere all'area Configurazione specifica del prodotto e impostare i campi seguenti:

- Giorni display non attivo
- Ora accensione display
- Durata accensione display
- Timeout display non attivo

Tabella 32: Campi di configurazione Risparmio energia

Campo	Descrizione
Giorni display non attivo	Giorni in cui il display non si accende automaticamente all'ora specificata nel campo Ora accensione display. Scegliere i giorni dall'elenco a discesa. Per scegliere più di un giorno, selezionare tutti i giorni desiderati tenendo premuto il tasto Ctrl.
Ora accensione display	L'ora in cui il display si accende automaticamente ogni giorno (tranne nei giorni specificati nel campo Giorni display non attivo). Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per accendere automaticamente il display alle 07:00, immettere **07:00**. Per accendere il display alle 14:00, immettere 14:00. (1400), immettere **14:00**. Se questo campo è vuoto, il display si accenderà automaticamente alle 00:00.
Durata accensione display	Intervallo di tempo in cui il display resta acceso dopo essersi acceso all'ora specificata nel campo Ora accensione display. Immettere in questo campo un valore nel formato *ore:minuti*. Ad esempio, per mantenere il display acceso per 4 ore e 30 minuti in seguito all'accensione automatica, immettere **04:30**. Se questo campo è vuoto, il telefono si spegnerà automaticamente alla fine della giornata (00:00). **Nota** Se per il campo Ora accensione display è stato immesso il valore 00:00 e per il campo della durata di accensione del display non è stato specificato nessun valore, (o è stato immesso il valore 24:00), il display resterà sempre acceso.

Campo	Descrizione
Timeout display non attivo	Intervallo di tempo in cui il telefono non è attivo prima dello spegnimento del display. Si applica solo se il display è stato acceso da un utente (tramite la pressione di un pulsante sul telefono o il sollevamento del ricevitore) mentre era spento in base alla pianificazione impostata. Immettere in questo campo un valore nel formato *ore:minuti*. Ad esempio, per spegnere il display dopo 1 ora e 30 minuti di inattività del telefono in seguito all'accensione del display da parte dell'utente, immettere **01:30**. Il valore predefinito è 01:00.

Passaggio 4 Selezionare **Salva**.

Passaggio 5 Selezionare **Applica configurazione**.

Passaggio 6 Riavviare il telefono.

Pianificazione di EnergyWise sul telefono IP Cisco

Se nel sistema è incluso un controller EnergyWise, per ridurre il consumo energetico configurare il telefono sulla sospensione (spegnimento) e sulla riattivazione (accensione).

Configurare le impostazioni in Cisco Unified Communications Manager Administration per abilitare EnergyWise e configurare gli orari di sospensione e riattivazione. Tali parametri sono strettamente collegati a quelli di configurazione del display del telefono.

Se EnergyWise è stato abilitato ed è stato impostato un orario di sospensione, il telefono invia allo switch una richiesta di riattivazione all'ora configurata. Lo switch risponde accettando o rifiutando la richiesta. Se lo switch rifiuta la richiesta o se non risponde, il telefono non si spegne. Se lo switch accetta la richiesta, il telefono inattivo va in modalità di sospensione, riducendo il consumo energetico fino a un livello preimpostato. Sui telefoni attivi viene impostato un timer di inattività alla scadenza del quale viene attivata la modalità di sospensione.

Per riattivare il telefono, premere Seleziona. All'ora di riattivazione pianificata, il sistema ripristina l'alimentazione sul telefono riattivandolo.

Per ulteriori informazioni, consultare Configurazione specifica del prodotto, a pagina 146

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono da impostare.

Passaggio 3 Accedere all'area Configurazione specifica del prodotto e impostare i campi seguenti.

- Abilita Power Save Plus
- Ora accensione telefono
- Ora spegnimento telefono
- Timeout inattività spegnimento telefono

- Abilita avviso acustico
- Dominio EnergyWise
- Segreto EnergyWise
- Consenti sostituzioni EnergyWise

Tabella 33: Campi di configurazione EnergyWise

Campo	Descrizione
Abilita Power Save Plus	Seleziona la pianificazione dei giorni in cui il telefono si spegne. Selezionare più giorni tenendo premuto il tasto Controllo e facendo contemporaneamente clic sui giorni da aggiungere alla pianificazione. Per impostazione predefinita, non è selezionato nessun giorno. Se il campo Abilita Power Save Plus è selezionato, si riceverà un messaggio di avviso sui problemi di ricezione delle chiamate di emergenza (e911). **Attenzione** Infatti, mentre la modalità Power Save Plus (la «Modalità») è attiva, gli endpoint configurati per questa modalità sono disabilitati per le chiamate di emergenza e per la ricezione delle chiamate in entrata. Selezionando questa modalità, si accetta quanto segue: (i) L'utente si assume la piena responsabilità nel fornire metodi alternativi per le chiamate di emergenza e la ricezione delle chiamate mentre questa modalità è attiva; (ii) Cisco declina ogni responsabilità relativamente alla scelta dell'utente di selezionare e abilitare la modalità (l'utente è l'unico responsabile); e (iii) L'amministratore accetta di informare gli utenti sulle conseguenze dell'attivazione della modalità sulle chiamate e sulle altre funzioni. **Nota** Per disabilitare Power Save Plus, è necessario deselezionare la casella di controllo Consenti sostituzioni EnergyWise. Se la casella Consenti sostituzioni EnergyWise rimane selezionata ma nel campo Abilita Power Save Plus non viene selezionato nessun giorno, la modalità Power Save Plus non viene disabilitata.
Ora accensione telefono	Determina l'ora di accensione automatica del telefono nei giorni indicati nel campo Abilita Power Save Plus. Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per accendere automaticamente il telefono alle 07:00 (0700), immettere 07:00. Per accendere il telefono alle 14:00 (1400), immettere 14:00. Il valore predefinito è vuoto e corrisponde alle 00:00. **Nota** I valori immessi nel campo Ora accensione telefono devono essere di almeno 20 minuti successivi a quelli immessi nel campo Ora spegnimento telefono. Ad esempio, se il valore immesso nel campo Ora spegnimento telefono è 07:00, il valore del campo Ora accensione telefono non deve essere precedente a 07:20.

Campo	Descrizione
Ora spegnimento telefono	L'ora in cui il telefono si spegne nei giorni selezionati nel campo Abilita Power Save Plus. Se nei campi Ora accensione telefono e Ora spegnimento telefono viene immesso lo stesso valore, il telefono non si spegne. Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte. Ad esempio, per spegnere automaticamente il telefono alle 7:00 (0700), immettere 7:00. Per spegnere il telefono alle 14:00 (1400), immettere 14:00. Il valore predefinito è vuoto e corrisponde alle 00:00. **Nota** I valori immessi nel campo Ora accensione telefono devono essere di almeno 20 minuti successivi a quelli immessi nel campo Ora spegnimento telefono. Ad esempio, se il valore immesso nel campo Ora spegnimento telefono è 07:00, il valore del campo Ora accensione telefono non deve essere precedente a 07:20.
Timeout inattività spegnimento telefono	Intervallo di tempo in cui il telefono resta inattivo prima di spegnersi. Il timeout si verifica nelle seguenti condizioni: • Quando la modalità Power Save Plus attivata sul telefono in base alla pianificazione viene disattivata perché l'utente preme il tasto **Seleziona**. • Quando il telefono viene riacceso dallo switch collegato. • Quando viene raggiunta l'ora di spegnimento del telefono ma il telefono è in uso. L'intervallo dei valori di questo campo va da 20 a 1440 minuti. Il valore predefinito è 60 minuti.
Abilita avviso acustico	Quando abilitato, invia al telefono l'istruzione di riprodurre un avviso acustico 10 minuti prima dell'ora specificata nel campo Ora spegnimento telefono. Per l'avviso acustico viene utilizzata la suoneria del telefono, riprodotta brevemente in momenti specifici durante l'intervallo di tempo di avviso di 10 minuti. La suoneria di avviso viene riprodotta al volume impostato dall'utente. La pianificazione dell'avviso acustico è la seguente: • 10 minuti prima dello spegnimento, la suoneria viene riprodotta per quattro volte. • 7 minuti prima dello spegnimento, la suoneria viene riprodotta per quattro volte. • 4 minuti prima dello spegnimento, la suoneria viene riprodotta per quattro volte. • 30 secondi prima dello spegnimento o fino allo spegnimento del telefono, la suoneria viene riprodotta per 15 volte. Questa casella di controllo viene applicata soltanto se nella casella Abilita Power Save Plus sono selezionati uno o più giorni.
Dominio EnergyWise	Dominio EnergyWise in cui si trova il telefono. La lunghezza massima di questo campo è di 127 caratteri.
Segreto EnergyWise	Password segreta di protezione utilizzata per comunicare con gli endpoint nel dominio EnergyWise. La lunghezza massima di questo campo è di 127 caratteri.

Campo	Descrizione
Consenti sostituzioni EnergyWise	Questa casella di controllo consente di stabilire se consentire al criterio del controller del dominio EnergyWise di inviare ai telefoni gli aggiornamenti sul livello di energia. Si applicano le condizioni seguenti: • Nel campo Abilita Power Save Plus devono essere selezionati uno o più giorni. • Le impostazioni configurate in Cisco Unified Communications Manager Administration vengono applicate alla pianificazione anche se EnergyWise invia una sostituzione. Ad esempio, presupporre che l'ora di spegnimento del telefono sia impostata sulle 22:00, che il valore specificato nel campo Ora accensione telefono sia 06:00 e che nel campo Abilita Power Save Plus siano presenti uno o più giorni selezionati. • Se EnergyWise invia al telefono il comando di spegnersi alle 20:00, questa istruzione rimane attiva (presupponendo che non vi sia alcun intervento da parte dell'utente) fino alle 06:00, ovvero fino all'ora configurata per l'accensione del telefono. • Alle 06:00, il telefono si accende e riprende la ricezione delle modifiche apportate al livello di energia dalle impostazioni di Unified Communications Manager Administration. • Per modificare nuovamente il livello di energia sul telefono, EnergyWise deve inviare un nuovo comando di modifica del livello di energia. **Nota** Per disabilitare Power Save Plus, è necessario deselezionare la casella di controllo Consenti sostituzioni EnergyWise. Se la casella Consenti sostituzioni EnergyWise rimane selezionata ma nel campo Abilita Power Save Plus non viene selezionato nessun giorno, la modalità Power Save Plus non viene disabilitata.

Passaggio 4 Selezionare **Salva**.

Passaggio 5 Selezionare **Applica configurazione**.

Passaggio 6 Riavviare il telefono.

Impostazione dell'opzione Non disturbare

Quando l'opzione Non disturbare (NoDist) è attiva, non è possibile udire la suoneria per le chiamate oppure non sono visibili né udibili notifiche di alcun tipo.

Quando la funzione Non disturbare (NoDist) è attivata, la sezione intestazione dello schermo del telefono cambia colore e sul telefono viene visualizzato `Non disturbare`.

È possibile configurare il telefono mediante un modello dei pulsanti del telefono con l'opzione NoDist come una delle funzioni selezionate.

Per ulteriori informazioni, consultare la sezione relativa alla funzione Non disturbare nella documentazione della versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono da configurare.

Passaggio 3 Impostare i parametri seguenti.

- Non disturbare: questa casella di controllo consente di abilitare la funzione NoDist sul telefono.
- Opzione NoDist: disattivazione della suoneria, rifiuto delle chiamate o impostazione Usa impostazione profilo telefono comune.

  Non scegliere il rifiuto delle chiamate se si desidera che le chiamate con priorità (MLPP) squillino su questo telefono quando la funzione NoDist è attivata.
- Allarme chiam in entrata NoDist: selezionare il tipo di avviso (facoltativo) da riprodurre sul telefono per segnalare le chiamate in arrivo quando è attiva l'opzione NoDist.

  Nota Questo parametro è disponibile nelle finestre Profilo telefono comune e Configurazione telefono. Il valore specificato nella finestra Configurazione telefono ha la precedenza.

Passaggio 4 Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Abilitazione della funzione Formula di apertura agente

La funzione Formula di apertura agente consente di creare e aggiornare un saluto preregistrato che viene riprodotto all'inizio di una chiamata, ad esempio una chiamata del cliente, prima che l'agente avvii la conversazione con il chiamante. In base alle necessità, l'agente può preregistrare una o più formule di apertura e crearle e aggiornarle.

Quando un cliente chiama, sia l'agente sia il chiamante ascoltano la formula di apertura preregistrata. L'agente può restare con il microfono disattivato fino al termine della formula di apertura o rispondere alla chiamata durante la riproduzione della stessa.

Tutti i codec supportati per il telefono sono supportati per le chiamate con la funzione Formula di apertura agente attivata.

Per ulteriori informazioni, consultare le sezioni relative alla privacy e all'inclusione nella documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono IP che si desidera configurare.

Passaggio 3 Scorrere fino al riquadro Layout informazioni dispositivo e impostare **Ponte incorporato** su On o su Predefinito.

Passaggio 4 Selezionare **Salva**.

Passaggio 5 Verificare l'impostazione del bridge:

a) Selezionare **Sistema** > **Parametri servizio**.
b) Selezionare il server e il servizio appropriati.
c) Scorrere fino al riquadro Parametri a livello di cluster (Dispositivo - Telefono) e impostare **Abilitazione bridge integrato** su On.
d) Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione della funzione di monitoraggio e registrazione

La funzione di monitoraggio e registrazione consente a un supervisore di monitorare una chiamata attiva in modalità invisibile. Le parti della chiamata non possono sentire il supervisore. L'utente potrebbe ricevere un avviso acustico durante una chiamata monitorata.

Se la chiamata è protetta, viene visualizzata un'icona di blocco. I chiamanti potrebbero inoltre ricevere un avviso acustico che indica che la chiamata è monitorata. Anche le parti connesse possono ricevere un avviso acustico che indica che la chiamata è protetta e monitorata.

Durante il monitoraggio o la registrazione di una chiamata attiva, l'utente può ricevere o effettuare delle chiamate tramite interfono; tuttavia, in questo caso, la chiamata attiva viene messa in attesa. Questa azione causa l'arresto della sessione di registrazione e la sospensione della sessione di monitoraggio. Per riprendere la sessione di monitoraggio, la persona monitorata deve riprendere la chiamata.

Per ulteriori informazioni, consultare la sezione relativa alla funzione di monitoraggio e registrazione nella documentazione della versione di Cisco Unified Communications Manager in uso.

Tramite la procedura riportata di seguito, è possibile aggiungere un utente ai gruppi utenti di monitoraggio standard.

Prima di iniziare

Per il supporto della funzione di monitoraggio e registrazione, è necessario che Cisco Unified Communications Manager sia configurato.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Gestione utente** > **Utente applicazione**.

Passaggio 2 Selezionare i gruppi utenti Consenti monitoraggio chiamate CTI standard e Consenti registrazione chiamate CTI standard.

Passaggio 3 Fare clic su **Aggiungi selezionati**.

Passaggio 4 Fare clic su **Aggiungi a gruppo di utenti**.

Passaggio 5 Aggiungere i telefoni degli utenti all'elenco dei dispositivi controllati degli utenti dell'applicazione.

Passaggio 6 Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione delle notifiche di deviazione chiamate

È possibile controllare le impostazioni di deviazione chiamate.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono da impostare.

Passaggio 3 Configurare i campi Notifica di deviazione chiamate.

Campo	Descrizione
Nome chiamante	Se questa casella di controllo è selezionata, nella finestra di notifica viene visualizzato il nome del chiamante. Per impostazione predefinita questa casella di controllo è selezionata.
Numero chiamante	Se questa casella di controllo è selezionata, nella finestra di notifica viene visualizzato il numero del chiamante. Per impostazione predefinita questa casella di controllo non è selezionata.
Numero reindirizzato	Se questa casella di controllo è selezionata, nella finestra di notifica vengono visualizzate le informazioni sull'ultimo chiamante che ha deviato la chiamata. Esempio: se il chiamante A chiama B, ma B ha deviato tutte le chiamate su C e C ha deviato tutte le chiamate su D, nella casella di notifica visualizzata da D vengono visualizzate le informazioni sul telefono del chiamante C. Per impostazione predefinita questa casella di controllo non è selezionata.
Numero composto	Se questa casella di controllo è selezionata, nella finestra di notifica vengono visualizzate le informazioni sul destinatario originale della chiamata. Esempio: se il chiamante A chiama B, ma B ha deviato tutte le chiamate su C e C ha deviato tutte le chiamate su D, nella casella di notifica visualizzata da D vengono visualizzate le informazioni sul telefono del chiamante B. Per impostazione predefinita questa casella di controllo è selezionata.

Passaggio 4 Selezionare **Salva**.

Abilitazione dell'indicatore di stato per elenchi chiamate

Il campo Indicatore distato per elenchi chiamate consente di controllare anche lo stato della linea per la funzione Rubrica aziendale.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Sistema** > **Parametri aziendali**.

Passaggio 2 Abilitare o disabilitare la funzione per il campo Indicatore di stato per elenchi chiamate.

Per impostazione predefinita, la funzione è disabilitata.

È possibile visualizzare i parametri impostati nell'area Configurazione specifica del prodotto anche nella finestra Configurazione dispositivo per diversi dispositivi e nella finestra Configurazione telefono aziendale. Se questi stessi parametri vengono impostati anche in queste altre finestre, l'ordine di precedenza delle impostazioni viene determinato nel modo seguente:

1. Impostazioni della finestra Configurazione dispositivo
2. Impostazioni della finestra Profilo telefono comune
3. Impostazioni della finestra Configurazione telefono aziendale

Passaggio 3 Selezionare **Salva**.

Impostazione di Energy Efficient Ethernet per la porta PC e dello switch

IEEE 802.3az Energy Efficient Ethernet (EEE) è un'estensione dello standard IEEE 802.3 che fornisce un metodo per ridurre il consumo di energia senza ridurre le funzioni principali delle interfacce di rete. Lo standard EEE configurabile consente all'amministratore di controllare le funzioni EEE sulla porta PC e dello switch.

Nota Per garantire il funzionamento dello standard EEE, gli amministratori devono verificare che la casella di controllo Sovrascrivi sia selezionata su tutte le pagine UCM applicabili.

L'amministratore controlla le funzioni EEE tramite i due parametri seguenti:

- **Energy Efficient Ethernet**: porta PC: fornisce connessione continua ai personal computer. L'amministratore può selezionare le opzioni Abilitato o Disabilitato per controllare la funzione.
- **Energy Efficient Ethernet**: porta dello switch: fornisce connessione continua.

Per ulteriori informazioni, consultareConfigurazione specifica del prodotto, a pagina 146

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare una delle finestre seguenti:

- **Dispositivo** > **Telefono**
- **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**
- **Sistema** > **Configurazione telefono aziendale**

Se si configura il parametro in più finestre, l'ordine di precedenza è:

1. **Dispositivo** > **Telefono**
2. **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**

3. **Sistema** > **Configurazione telefono aziendale**

Passaggio 2 Se richiesto, individuare il telefono.

Passaggio 3 Impostare i campi **Energy Efficient Ethernet: porta PC** e **Energy Efficient Ethernet: porta dello switch**.

- Energy Efficient Ethernet: porta PC
- Energy Efficient Ethernet: porta dello switch

Passaggio 4 Selezionare **Salva**.

Passaggio 5 Selezionare **Applica configurazione**.

Passaggio 6 Riavviare il telefono.

Impostazione dell'intervallo di porta RTP/sRTP

Configurare i valori della porta Real-Time Transport Protocol (RTP) e secure Real-Time Transport Protocol (sRTP) nel profilo SIP. L'intervallo dei valori della porta RTP e sRTP va da 2048 a 65535 con un intervallo predefinito compreso tra 16384 e 32764. Alcuni valori della porta all'interno dell'intervallo di porta RTP e sRTP sono progettati per altri servizi telefonici. Non è possibile configurare queste porte per RST e sRTP.

Per ulteriori informazioni, consultare la sezione relativa al profilo SIP nella documentazione della versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo SIP**.

Passaggio 2 Scegliere i criteri di ricerca da utilizzare e fare clic su **Trova**.

Passaggio 3 Selezionare il profilo da modificare.

Passaggio 4 Impostare i campi Porta iniziale media e Porta finale media in modo che contengano l'inizio e la fine dell'intervallo di porta.

Nell'elenco seguente vengono identificate le porte UDP utilizzate per altri servizi telefonici e pertanto non disponibili per l'uso con RTP e sRTP:

porta 4051

utilizzata per la funzione Condivisione del firmware (PFS)

porta 5060

utilizzata per SIP su trasporto UDP

intervallo di porta da 49152 a 53247

utilizzato per le porte temporanee locali

intervallo di porta da 53248 a 65535

utilizzato per la funzione VPN tunnel singolo VXC

Passaggio 5 Fare clic su **Salva**.

Passaggio 6 Fare clic su **Applica configurazione**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway(MRA) consente ai lavoratori remoti di connettersi con facilità e in sicurezza alla rete aziendale senza utilizzare un tunnel client VPN (Virtual Private Network). Expressway utilizza TLS (Transport Layer Security) per la protezione del traffico di rete. Per fare in modo che il telefono autentichi un certificato Expressway e stabilisca una sessione TLS, un'autorità di certificazione pubblica ritenuta attendibile dal firmware del telefono deve firmare il certificato Expressway. Non è possibile installare o considerare attendibili altri certificati CA sui telefoni per l'autenticazione di un certificato Expressway.

L'elenco dei certificati CA integrati nel firmware del telefono è disponibile all'indirizzo http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

Mobile and Remote Access Through Expressway (MRA) funziona con Cisco Expressway. pertanto è consigliabile avere dimestichezza con la documentazione di Cisco Expressway, inclusa la *Guida dell'amministratore di Cisco Expressway* e la *Guida alla distribuzione della configurazione di base di Cisco Expressway*. La documentazione di Cisco Expressway è disponibile all'indirizzo http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Per gli utenti di Mobile and Remote Access Through Expressway, è supportato soltanto il protocollo IPv4.

Per ulteriori informazioni sull'uso di Mobile and Remote Access Through Expressway, consultare:

- *Cisco Preferred Architecture for Enterprise Collaboration, Panoramica sulla progettazione*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Guida alla distribuzione di Unified Communications Mobile and Remote Access tramite Cisco VCS*
- *Cisco TelePresence Video Communication Server (VCS), Guide alla configurazione*
- *Guida all'implementazione dell'accesso mobile e remoto tramite Cisco Expressway*

Durante il processo di registrazione del telefono, quest'ultimo effettua la sincronizzazione della data e dell'ora visualizzate con il server Network Time Protocol (NTP). Con MRA, l'etichetta dell'opzione 42 DHCP viene utilizzata per individuare gli indirizzi IP dei server NTP designati per la sincronizzazione della data e dell'ora. Se nelle informazioni sulla configurazione non è possibile individuare l'etichetta dell'opzione 42 DHCP, per identificare i server NTP il telefono cerca l'etichetta 0.tandberg.pool.ntp.org.

In seguito alla registrazione, il telefono utilizza le informazioni contenute nel messaggio SIP per sincronizzare la data e l'ora visualizzate a meno che nella configurazione del telefono di Cisco Unified Communications Manager non sia configurato un server NTP.

Nota Se nel profilo di sicurezza di uno dei telefoni in uso è stata selezionata l'opzione Config TFTP crittografata, non sarà possibile utilizzare il telefono con accesso mobile e remoto. La soluzione MRA non supporta l'interazione del dispositivo con CAPF (Certificate Authority Proxy Function).

Mobile and Remote Access Through Expressway supporta la modalità linea avanzata.

La modalità SIP OAuth è supportata per MRA. Questa modalità consente di utilizzare i token di accesso OAuth per l'autenticazione in ambienti sicuri.

Nota Per SIP OAuth in modalità MRA (Mobile and Remote Access), utilizzare solo l'onboarding con codice di attivazione con MRA durante la distribuzione del telefono. Non è supportata l'attivazione con nome utente e password.

La modalità SIP OAuth richiede Expressway x14.0(1) e versioni successive o Cisco Unified Communications Manager 14.0(1) e versioni successive.

Per ulteriori informazioni sulla modalità SIP OAuth, vedere la *Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager* versione 14.0(1) o successive.

Scenari di distribuzione

Nella tabella seguente vengono presentati diversi scenari di implementazione per Mobile and Remote Access Through Expressway.

L'utente in sede accede alla rete aziendale

Dopo aver distribuito Mobile and Remote Access Through Expressway, l'utente deve eseguire l'accesso alla rete aziendale quando si trova in sede. Il telefono rileva la rete e si registra su Cisco Unified Communications Manager.

L'utente fuori sede accede alla rete aziendale

Quando l'utente non è in ufficio, il telefono rileva di essere in modalità fuori sede. Viene visualizzata la finestra Accedi di Mobile and Remote Access Through Expressway e l'utente si connette alla rete aziendale.

Tenere presente quanto segue:

- L'utente deve disporre di un dominio di servizio, un nome utente e una password validi per collegarsi alla rete.
- Prima di poter accedere alla rete aziendale, l'utente deve inoltre ripristinare la modalità di servizio per cancellare l'impostazione TFTP alternativo. In questo modo, viene cancellata l'impostazione Server TFTP alternativo in modo che il telefono possa individuare la rete fuori sede e impedire al telefono di stabilire una connessione VPN. Ignorare questo passaggio se è in corso la prima distribuzione del telefono.
- Se l'utente ha un'opzione DHCP 150 o 66 abilitata sul router di rete, potrebbe non riuscire ad accedere alla rete aziendale. Per attivare la modalità MRA, reimpostare la modalità di servizio.

L'utente fuori sede accede alla rete aziendale con la VPN

Se è fuori sede, l'utente deve accedere alla rete aziendale con la VPN, dopo la distribuzione di Mobile and Remote Access Through Expressway.

In caso di errore, eseguire una reimpostazione di base della configurazione del telefono.

È necessario configurare l'impostazione TFTP alternativo (**Impostazioni amministratore** > **Impostazioni di rete** > **IPv4**, campo **Server TFTP alternativo 1**).

Argomenti correlati

Reimpostazione di base, a pagina 277

Percorsi di supporti e Interactive Connectivity Establishment

È possibile distribuire Interactive Connectivity Establishment (ICE) per migliorare l'affidabilità delle chiamate tramite MRA (Mobile and Remote Access) instradate tramite un firewall o Network Address Translation (NAT). ICE è una distribuzione opzionale che utilizza Serial Tunnel (STUN) e Traversal Using Relays around NAT (TURN) per selezionare il migliore percorso del supporto per una chiamata.

Non sono supportati un server TURN secondario e il failover del server TURN.

Per ulteriori informazioni su MRA e ICE, consultare la *Guida alla configurazione del sistema di Cisco Unified Communications Manager versione 12.0(1)* o successive. È inoltre possibile trovare ulteriori informazioni nei documenti Richiesta di commenti (RFC) di IEFT (Internet Engineering Task Force):

- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols* (RFC 5245)

Funzioni del telefono disponibili per Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway offre accesso sicuro senza VPN ai servizi di collaborazione per gli utenti remoti e di dispositivi mobili Cisco. Tuttavia, per garantire la sicurezza della rete, limita l'accesso alle funzioni del telefono.

Nell'elenco che segue sono indicate le funzioni del telefono disponibili con Mobile and Remote Access Through Expressway.

Tabella 34: Supporto funzioni e Mobile and Remote Access Through Expressway

Funzione del telefono	Versione del firmware del telefono
Composizione abbreviata	10.3(1) e successive
Rispondi alla meno recente	11.5(1)SR1 e successive
Parcheggio chiamata indirizzato assistito	10.3(1) e successive
Risposta automatica	11.5(1)SR1 e successive
Inclusione e Incl_m	11.5(1)SR1 e successive
Indicatore di stato	10.3(1) e successive
Risposta per assente con indicatore di stato della linea	10.3(1) e successive
Chiamata rapida con indicatore di stato	10.3(1) e successive
Prenotazione di chiamata	10.3(1) e successive
Inoltro di chiamata	10.3(1) e successive
Notifica di inoltro di chiamata	10.3(1) e successive

Funzione del telefono	Versione del firmware del telefono
Parcheggio chiamata	10.3(1) e successive
Risposta per assente	10.3(1) e successive
Servizi Cisco Unified	11.5(1)SR1 e successive
Licenza CAL (Client Access License)	11.5(1)SR1 e successive
Conferenza	10.3(1) e successive
Elenco partecipanti conferenza/Rimuovi partecipante	11.5(1)SR1 e successive
Rubrica aziendale	11.5(1)SR1 e successive
Applicazioni CTI (controllate da CTI)	11.5(1)SR1 e successive
Trasferimento diretto	10.3(1) e successive
Parcheggio chiamata indirizzato	10.3(1) e successive
Suoneria distintiva	11.5(1)SR1 e successive
Devia	10.3(1) e successive
Modalità linea avanzata	12.1(1) e successive
Devia	10.3(1) e successive
Codici di accesso forzato e Codici distintivi cliente	11.5(1)SR1 e successive
Risposta per assente di gruppo	10.3(1) e successive
Attesa/Riprendi	10.3(1) e successive
Ripristino attesa	10.3(1) e successive
Deviazione immediata	10.3(1) e successive
Collega	10.3(1) e successive
Identificazione chiamate indesiderate (MCID, Malicious Call Identification)	11.5(1)SR1 e successive
Conferenza automatica	10.3(1) e successive
Indicatore di messaggio in attesa	10.3(1) e successive
Connessione mobile	10.3(1) e successive
Accesso vocale mobile	10.3(1) e successive
MLPP (Multilevel Precedence and Preemption, Precedenza e prelazione multilivello)	11.5(1)SR1 e successive
Telefono IP	11.5(1)SR1 e successive

Funzione del telefono	Versione del firmware del telefono
Musica di attesa	10.3(1) e successive
Disattiva audio	10.3(1) e successive
Profili di rete (automatici)	11.5(1)SR1 e successive
Composizione con ricevitore sganciato	10.3(1) e successive
Composizione con ricevitore agganciato	10.3(1) e successive
Composizione di un numero con il segno + (più)	10.3(1) e successive
Privacy	11.5(1)SR1 e successive
Private Line Automated Ringdown (PLAR)	11.5(1)SR1 e successive
Ripeti	10.3(1) e successive
Chiamata rapida (non supporta una pausa)	10.3(1) e successive
Pulsante URL servizi	11.5(1)SR1 e successive
Trasferisci	10.3(1) e successive
Composizione URI (Uniform Resource Identifier)	10.3(1) e successive

Configurazione di credenziali utente persistenti per l'accesso a Expressway

Quando effettua l'accesso alla rete con Mobile and Remote Access Through Expressway, all'utente viene richiesto di specificare il dominio, il nome utente e la password del servizio. Se si abilita il parametro Credenziali utente persistenti per l'accesso a Expressway, le credenziali di accesso dell'utente vengono memorizzate in modo tale che non sia più necessario immetterle nuovamente. Questo parametro è disabilitato per impostazione predefinita.

È possibile impostare le credenziali in modo permanente per un telefono singolo, un gruppo di telefoni o tutti i telefoni.

Argomenti correlati

Configurazione delle funzioni del telefono, a pagina 144
Configurazione specifica del prodotto, a pagina 146

Creazione di un codice QR per l'accesso MRA

Gli utenti con un telefono dotato di videocamera possono effettuare la scansione di un codice QR per accedere a MRA invece di immettere manualmente il dominio di servizio e il nome utente.

Procedura

Passaggio 1 Utilizzare un generatore di codici QR per generare un codice QR con il dominio di servizio o con il dominio di servizio e il nome utente separati da una virgola. Ad esempio: mra.example.com o mra.example.com,username.

Passaggio 2 Stampare il codice QR e inviarlo all'utente.

Problem Reporting Tool (PRT)

Tramite Cisco Collaboration Problem Reporting Tool, gli utenti inviano le segnalazioni dei problemi.

Nota Durante le operazioni di risoluzione dei problemi, Cisco TAC (Technical Assistance Center) richiede i registri di Cisco Collaboration Problem Reporting Tool. I registri vengono cancellati se si riavvia il telefono. Raccogliere i registri prima di riavviare i telefoni.

Per inviare una segnalazione di un problema, gli utenti accedono a Cisco Collaboration Problem Reporting Tool e inseriscono la data e l'ora in cui si è verificato il problema insieme a una sua descrizione.

Se il caricamento PRT non riesce, è possibile accedere al file PRT per il telefono dall'URL **`http://<phone-ip-address>/FS/<prt-file-name>`**. Questo URL viene visualizzato sul telefono nei casi seguenti:

- Se il telefono è ancora nello stato predefinito di fabbrica. L'URL rimane attivo per 1 ora. Dopo 1 ora, sarà necessario provare a inviare nuovamente i registri del telefono.
- Se il telefono ha scaricato un file di configurazione e il sistema di controllo delle chiamate consente l'accesso Web al telefono.

È necessario aggiungere un indirizzo del server al campo **URL di caricamento supporto tecnico ai clienti** su Cisco Unified Communications Manager.

In caso di distribuzione dei dispositivi con Mobile and Remote Access through Expressway, è necessario inoltre aggiungere l'indirizzo del server PRT all'elenco degli indirizzi autorizzati del server HTTP sul server Expressway.

Configurazione di un URL di caricamento assistenza clienti

Per ricevere i file PRT, è necessario utilizzare un server con uno script di caricamento. Il file PRT utilizza un meccanismo HTTP POST, con i parametri seguenti inclusi nel caricamento (tramite la codifica MIME a più parti):

- devicename (esempio: «SEP001122334455»)
- serialno (esempio: «FCH12345ABC»)
- username (il nome utente configurato in Cisco Unified Communications Manager, il proprietario del dispositivo)
- prt_file (esempio: «probrep-20141021-162840.tar.gz»)

Di seguito è riportato uno script di esempio. Lo script viene fornito soltanto come riferimento. Cisco non fornisce supporto per lo script di caricamento installato sul server del cliente.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
```

```
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Nota I telefoni supportano solo gli URL HTTP.

Procedura

Passaggio 1 Impostare un server in grado di eseguire lo script di caricamento PRT.

Passaggio 2 Scrivere uno script in grado di gestire i parametri elencati sopra oppure modificare lo script di esempio fornito in base alle proprie esigenze.

Passaggio 3 Caricare lo script sul server.

Passaggio 4 In Cisco Unified Communications Manager, andare all'area Layout configurazione specifica del prodotto della finestra di configurazione del singolo dispositivo, della finestra Profilo telefono comune o della finestra Configurazione telefono aziendale.

Passaggio 5 Selezionare **URL di caricamento del supporto tecnico ai clienti** e immettere l'URL del server di caricamento.

Esempio:

http://example.com/prtscript.php

Passaggio 6 Salvare le modifiche.

Impostazione di un'etichetta per una linea

È possibile impostare un telefono sulla visualizzazione di un'etichetta di testo al posto del numero di rubrica. Utilizzare questa etichetta per identificare la linea in base al nome o alla funzione. Ad esempio, se l'utente

condivide delle linee sul telefono, è possibile identificare la linea con il nome della persona con cui si condivide tale linea.

Quando si aggiunge un'etichetta a un modulo di espansione tasti, su una linea vengono visualizzati solo i primi 25 caratteri.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.
Passaggio 2	Individuare il telefono da configurare.
Passaggio 3	Individuare l'istanza della linea e impostare il campo Etichetta di testo della linea.
Passaggio 4	(Facoltativo) Se è necessario applicare l'etichetta ad altri dispositivi che condividono la linea, selezionare la casella di controllo Aggiorna impostazioni dispositivo condiviso e fare clic su **Propaga impostazioni selezionate**.
Passaggio 5	Selezionare **Salva**.

Impostazione delle informazioni Dual Bank

Per impostare le informazioni Dual Bank, attenersi alla procedura seguente:

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Valori predefiniti dispositivo**.
Passaggio 2	Verificare le informazioni sul carico nel campo Informazioni carico inattivo.
Passaggio 3	Selezionare **Amministrazione globale** > **Importa/Esporta** > **Esporta** > **Valori predefiniti dispositivo** e programmare un processo di esportazione.
Passaggio 4	Scaricare il file .tar esportato e decomprimerlo.
Passaggio 5	Controllare il formato di file del file CSV esportato e verificare che nel file CSV sia presente la colonna Informazioni carico inattivo contenente il valore corretto.

Nota Il valore del file CSV deve corrispondere al valore specificato per Valore predefinito dispositivo nella finestra di Cisco Unified Communications Manager Administration.

Monitoraggio parcheggio

La funzione di parcheggio chiamata è supportata solo quando una chiamata viene parcheggiata sul telefono IP Cisco. La funzione di parcheggio chiamata monitora quindi lo stato della chiamata parcheggiata. Il fumetto del parcheggio chiamata rimane visualizzato finché la chiamata parcheggiata non viene recuperata o abbandonata. È possibile recuperare la chiamata parcheggiata utilizzando lo stesso fumetto della chiamata sul telefono su cui tale chiamata è stata parcheggiata.

Impostazione dei timer di Park Monitoring

In Cisco Unified Communications Manager Administration sono disponibili tre parametri per il timer del servizio a livello di cluster per il monitoraggio del parcheggio: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer e Park Monitoring Forward No Retrieve Timer. Ciascun parametro del servizio include un valore predefinito e non richiede nessuna configurazione speciale. Tali parametri del timer si applicano esclusivamente al monitoraggio del parcheggio; i timer di visualizzazione del parcheggio chiamata e di ripristino del parcheggio chiamata non vengono utilizzati per il monitoraggio del parcheggio. Per le descrizioni di questi parametri, consultare la tabella seguente.

Configurare i timer nella pagina Parametri servizio di Cisco Unified Communications Manager.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Sistema** > **Parametri servizio**.

Passaggio 2 Aggiornare i campi Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer e Park Monitoring Forward No Retrieve Timer nel riquadro Parametri a livello di cluster (Funzione - Generale).

Tabella 35: Parametri servizio per monitoraggio parcheggio

Campo	Descrizione
Park Monitoring Reversion Timer	L'impostazione predefinita è 60 secondi. Questo parametro determina l'intervallo di tempo e secondi che devono trascorrere prima che Cisco Unified Communications Manager richieda recuperare una chiamata parcheggiata. Questo timer si avvia quando l'utente preme Parcheg telefono e alla sua scadenza viene visualizzato un promemoria. È possibile ignorare il valore specificato da questo parametro del servizio su ciascuna linea Monitoraggio parcheggio della finestra Configurazione numero di rubrica (in Cisco Unified Co Manager Administrations, selezionare **Indirizzamento chiamata** > **Nr. di rubrica**). Specifi pari a 0 per utilizzare immediatamente l'intervallo di ripristino periodico specificato dal para servizio Park Monitoring Periodic Reversion Timer (vedere la descrizione seguente). Ad esem parametro è impostato su zero e Park Monitoring Periodic Reversion Timer è impostato su viene chiesto se riprendere la chiamata parcheggiata immediatamente e successivamente og fino alla scadenza di Park Monitoring Forward No Retrieve Timer (vedere la descrizione se
Park Monitoring Periodic Reversion Timer	L'impostazione predefinita è 30 secondi. Questo parametro determina l'intervallo di tempo (secondi) che deve trascorrere prima che Cisco Unified Communications Manager ricordi nu all'utente che è presente una chiamata parcheggiata. Per connettersi alla chiamata parcheggi può semplicemente sollevare il ricevitore durante la visualizzazione di uno di questi prompt chiamata rimane parcheggiata e fino alla scadenza dell'intervallo specificato da Park Monito No Retrieve Timer, Cisco Unified Communications Manager continua a ricordare all'utente una chiamata parcheggiata (vedere la descrizione seguente). Specificare un valore pari a 0 p i prompt periodici sulla chiamata parcheggiata.

Campo	Descrizione
Park Monitoring Forward No Retrieve Timer	L'impostazione predefinita è 300 secondi. Questo parametro determina l'intervallo di tempo esp secondi in cui vengono visualizzate le notifiche di promemoria sul parcheggio prima che la chia parcheggiata venga deviata alla destinazione Park Monitoring Forward No Retrieve specificata nel Configurazione numero di rubrica dell'utente che ha parcheggiato la chiamata (se in Cisco Unif Communications Manager Administration non viene specificata nessuna destinazione di deviaz chiamata ritorna alla linea su cui è stata parcheggiata). Questo parametro si avvia alla scadenza dell specificato dal parametro del servizio Park Monitoring Reversion Timer. Alla scadenza di Park M Forward No Retrieve Timer, la chiamata viene rimossa dal parcheggio e viene deviata sulla des specificata o ripristinata sulla linea dell'utente che l'ha parcheggiata.

Impostazione dei parametri di Park Monitoring per i numeri di rubrica

Nella finestra Configurazione numero di rubrica è presente un'area Park Monitoring in cui è possibile configurare i tre parametri.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Indirizzamento chiamata** > **Nr. di rubrica**.

Passaggio 2 Impostare i campi di monitoraggio del parcheggio come descritto nella tabella seguente.

Tabella 36: Parametri di Park Monitoring

Campo	Descrizione
Park Monitoring Forward No Retrieve Destination External	Se l'utente della chiamata parcheggiata è una parte esterna, la chiamata viene deviata alla destinazione specificata nel parametro Park Monitoring Forward No Retrieve Destination External dell'utente che ha parcheggiato la chiamata. Se il valore del campo Forward No Retrieve Destination External è vuoto, l'utente della chiamata parcheggiata viene reindirizzato alla linea dell'utente che ha parcheggiato la chiamata.
Park Monitoring Forward No Retrieve Destination Internal	Se l'utente della chiamata parcheggiata è una parte interna, la chiamata viene deviata alla destinazione specificata nel parametro Park Monitoring Forward No Retrieve Destination Internal dell'utente che ha parcheggiato la chiamata. Se il campo Forward No Retrieve Destination Internal è vuoto, l'utente della chiamata parcheggiata viene reindirizzato alla linea dell'utente che ha parcheggiato la chiamata.

Campo	Descrizione
Park Monitoring Reversion Timer	Questo parametro determina l'intervallo di tempo espresso in secondi che devono trascorrere prima che Cisco Unified Communications Manager richieda all'utente di recuperare una chiamata parcheggiata. Questo timer si avvia quando l'utente preme ParchegChiam sul telefono e alla sua scadenza viene visualizzato un promemoria. Impostazione predefinita: 60 secondi Il valore del parametro impostato nella finestra Parametri servizio viene sovrascritto se si configura un valore diverso da zero. Tuttavia, se viene configurato un valore pari a 0, viene utilizzato il valore impostato nella finestra Parametri servizio.

Impostazione del monitoraggio parcheggio per gli elenchi di ricerca

Quando una chiamata indirizzata tramite l'elenco di ricerca viene parcheggiata, alla scadenza del parametro Monitoraggio parcheggio Inoltra N. Recupera timer viene utilizzato il valore del parametro Pilot di ricerca Monitoraggio parcheggio Inoltra N. Recupera destinazione (a meno che non sia vuoto).

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Indirizzamento chiamata** > **Route/Hunt** > **Pilot di ricerca**.

Passaggio 2 Impostare il parametro Pilot di ricerca Monitoraggio parcheggio Inoltra N. Recupera destinazione.

Se il valore del parametro Hunt Pilot Park Monitoring Forward No Retrieve Destination è vuoto, alla scadenza di Park Monitoring Forward No Retrieve Timer, la chiamata viene inoltrata alla destinazione configurata nella finestra Configurazione numero di rubrica.

Impostazione dell'intervallo di porta audio e video

Per migliorare la qualità del servizio (QoS), è possibile inviare il traffico audio e video a più intervalli di porta RTP.

È possibile controllare gli intervalli di porta in Cisco Unified Communications Manager Administration tramite i campi seguenti:

- Porte audio
  - Porta iniziale media (predefinita: 16384)
  - Porta finale media (predefinita: 32766)
- Porte video
  - Video iniziale (per impostare la porta iniziale video)

- Minimo: 2048
- Massimo: 65535

- Video finale (per impostare la porta finale video)
  - Minimo: 2048
  - Massimo: 65535

Per la configurazione dei campi della porta video, si applicano le regole seguenti:

In seguito alla configurazione della porta iniziale RTP video e della porta finale RTP video, il telefono utilizza le porte all'interno dell'intervallo di porte video per il traffico video. Per il traffico audio vengono utilizzate le porte multimediali.

Se gli intervalli delle porte audio e video si sovrappongono, le porte sovrapposte trasmettono sia il traffico video che il traffico audio. Se l'intervallo della porta video non è configurato correttamente, il telefono utilizza le porte audio configurate sia per il traffico video che per il traffico audio.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Profilo SIP**.

Passaggio 2 Impostare i campi Porta iniziale media e Porta finale media per l'intervallo della porta audio.

Passaggio 3 Selezionare **Salva**.

Passaggio 4 Selezionare una delle finestre seguenti:

- **Sistema** > **Configurazione telefono aziendale**
- **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**
- **Dispositivo** > **Telefono** > **Configurazione telefono**

Passaggio 5 Impostare i campi Porta iniziale RTP video e Porta finale RTP video sull'intervallo di porte richiesto.

Per la configurazione dei campi della porta video, si applicano le regole seguenti:

- Il valore del campo Porta finale RTP video deve essere superiore a quello specificato nel campo Porta iniziale RTP video.
- La differenza tra i campi Porta iniziale RTP video e Porta finale RTP video deve essere di almeno 16.

Passaggio 6 Selezionare **Salva**.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione di Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) fornisce funzioni di indirizzamento chiamata e altre funzioni che consentono ai direttori e agli assistenti di gestire le chiamate in modo più efficace.

È necessario configurare i servizi IPMA in Cisco Unified Communications Manager per consentire di utilizzarli. Per informazioni dettagliate sulla configurazione di IPMA, vedere la *Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager*.

IPMA è costituito da tre pulsanti:

Direttore

Al direttore vengono rilevate le chiamate in arrivo tramite il servizio di instradamento delle chiamate.

Assistente

L'assistente gestisce le chiamate per conto di un direttore.

Assistant Console

L'Assistant Console è un'applicazione desktop che può essere utilizzata dagli assistenti per eseguire attività e gestire la maggior parte delle funzioni.

IPMA supporta due modalità operative: supporto della linea proxy e supporto della linea condivisa. Entrambe le modalità supportano più chiamate per linea del direttore. Il servizio IPMA supporta sia la linea proxy che la linea condivisa in un cluster.

Nella modalità di linea condivisa, il direttore e l'assistente condividono un numero di rubrica e le chiamate vengono gestite sulla linea condivisa. Quando una chiamata viene ricevuta sulla linea condivisa, squilla sia il telefono del direttore che quello dell'assistente. La modalità di linea condivisa non supporta le funzioni Selezione assistente predefin., Controllo Assistente, il filtro delle chiamate o la deviazione di tutte le chiamate.

Se si configura Cisco IPMA nella modalità di linea condivisa, il direttore e l'assistente condividono il numero di rubrica, ad esempio 1701. L'assistente gestisce le chiamate del direttore sul numero di rubrica condiviso. Quando un direttore riceve una chiamata sul numero di rubrica 1701, il telefono del direttore e quello dell'assistente squillano in contemporanea.

Nella modalità di linea condivisa non sono disponibili tutte le funzioni IPMA, inclusi la selezione dell'assistente predefinito, il controllo dell'assistente, il filtro delle chiamate e la deviazione di tutte le chiamate. Un assistente non può visualizzare né accedere a queste funzioni dall'applicazione Assistant Console. Il telefono dell'assistente non dispone della softkey per la funzione Devia Tutte. Il telefono del direttore non dispone delle softkey per le funzioni Controllo Assistente, Intercettazione chiamate o Devia Tutte.

Per accedere al supporto della linea condivisa sui dispositivi degli utenti, è necessario innanzitutto configurare e avviare il servizio Cisco IP Manager Assistant tramite Cisco Unified Communications Manager Administration.

Nella modalità di linea proxy, l'assistente gestisce le chiamate per conto del direttore tramite un numero proxy. La modalità di linea proxy supporta tutte le funzioni IPMA.

Se l'amministratore configura Cisco IPMA nella modalità di linea proxy, il direttore e l'assistente non condividono un numero di rubrica. L'assistente gestisce le chiamate per conto del direttore tramite un numero proxy. Il numero proxy non corrisponde al numero di rubrica del direttore, ma è un numero alternativo scelto dal sistema e utilizzato dall'assistente per la gestione delle chiamate del direttore. In modalità di linea proxy, un direttore e un assistente possono accedere a tutte le funzioni disponibili in IPMA, inclusi la selezione dell'assistente predefinito, il controllo dell'assistente, il filtro delle chiamate e la deviazione di tutte le chiamate.

Per accedere al supporto della linea proxy sui dispositivi degli utenti, è necessario innanzitutto configurare e avviare il servizio Cisco IP Manager Assistant tramite Cisco Unified Communications Manager Administration.

È possibile accedere alle funzioni IPMA tramite le softkey e i servizi telefonici. Il modello delle softkey è configurato su Cisco Unified Communications Manager. IPMA supporta i seguenti modelli delle softkey standard:

Direttore standard

Supporta il direttore per la modalità proxy.

Direttore modalità condivisa standard

Supporta il direttore per la modalità condivisa.

Assistente standard

Supporta l'assistente nella modalità proxy o condivisa.

Nella tabella seguente vengono descritte le softkey disponibili nel modello delle softkey.

Tabella 37: Softkey IPMA

Softkey	Stato della chiamata	Descrizione
Reindirizza	Chiamata in arrivo, Connessa, In attesa	Devia la chiamata selezionata a una destinazione preconfigurata.
Intercetta	Tutti gli stati	Devia una chiamata dal telefono dell'assistente al telefono del direttore rispondendo automaticamente.
Controlla Assistente	Tutti gli stati	Visualizza lo stato della chiamata gestita da un assistente.
TrasfCv	Chiamata in arrivo, Connessa, In attesa	Reindirizza la chiamata selezionata alla casella vocale del direttore.
Devia Tutte	Tutti gli stati	Devia tutte le chiamate indirizzate al direttore su una destinazione preconfigurata.

Nota È consigliabile configurare le funzioni Intercetta, Controlla Assistente e Devia Tutte sul telefono del direttore soltanto nella modalità di linea proxy.

Nella procedura riportata di seguito viene riportata una panoramica dei passaggi richiesti.

Procedura

Passaggio 1 Configurare i telefoni e gli utenti.

Passaggio 2 Associare i telefoni agli utenti.

Passaggio 3 Attivare il servizio Cisco IP Manager Assistant nella finestra Attivazione del servizio.

Passaggio 4 Configurare i parametri di amministrazione del sistema.

Passaggio 5	Se necessario, configurare i parametri dei servizi IPMA a livello di cluster.
Passaggio 6	(Facoltativo) Configurare il profilo CAPF dell'utente.
Passaggio 7	(Facoltativo) Configurare i parametri dei servizi IPMA per la protezione.
Passaggio 8	Arrestare e riavviare il servizio IPMA.
Passaggio 9	Configurare le impostazioni del parametro del telefono, del direttore e dell'assistente, inclusi i modelli delle softkey.
Passaggio 10	Configurare l'applicazione Cisco Unified Communications Manager Assistant.
Passaggio 11	Configurare le regole di composizione.
Passaggio 12	Installare l'applicazione Assistant Console.
Passaggio 13	Configurare le applicazioni Manager e Assistant Console.

Impostazione di Visual Voicemail

Visual Voicemail viene configurato per tutti i telefoni IP Cisco o su un utente singolo o un gruppo di utenti da Cisco Unified Communications Manager Administration.

Nota Per le informazioni di configurazione, consultare la documentazione relativa a Cisco Visual Voicemail all'indirizzo http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Il client di Visual Voicemail non è supportato come midlet su nessuno dei telefoni IP Cisco serie 8800.

Procedura

Passaggio 1	In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Servizi telefonici**.
Passaggio 2	Selezionare **Aggiungi nuovo** per creare un nuovo servizio per Visual Voicemail.
Passaggio 3	Nella finestra Configurazione servizi telefono IP immettere le seguenti informazioni nei rispettivi campi: • Nome servizio: immettere **`VisualVoiceMail`**. • Nome servizio ASCII: immettere **`VisualVoiceMail`**. • URL servizio: immetterlo nel formato **`Applicazione:Cisco/VisualVoiceMail`**. • Categoria servizio: selezionare **Servizio XML** dal menu a discesa. • Tipo di servizio: selezionare **Messaggi** nel menu a discesa.
Passaggio 4	Selezionare **Abilita** e fare clic su **Salva**. **Nota** Assicurarsi di non selezionare **Iscrizione aziendale**.
Passaggio 5	Nella finestra Informazioni parametro servizio, fare clic su **Nuovo parametro** e immettere le informazioni seguenti nei rispettivi campi: • Nome parametro. Immettere voicemail_server. • Nome visualizzato del parametro. Immettere voicemail_server. • Valore predefinito. Immettere il nome host del server Unity primario.

- Descrizione parametro.

Passaggio 6 Selezionare **Parametro obbligatorio** e fare clic su **Salva**.

Nota Assicurarsi di non selezionare **Il parametro è una password (maschera contenuti)**.

Passaggio 7 Chiudere la finestra e selezionare nuovamente **Salva** nella finestra Configurazione servizio telefonico.

Impostazione di Visual Voicemail per un utente specifico

Attenersi alla procedura seguente per configurare Visual Voicemail per un utente specifico.

Nota Per le informazioni di configurazione, consultare la documentazione relativa a Cisco Visual Voicemail all'indirizzo http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Selezionare il dispositivo associato all'utente che si sta cercando.

Passaggio 3 Nel menu a discesa Collegamenti correlati, selezionare **Sottoscrivi/Annulla sottoscrizione ai servizi** e fare clic su **Vai**.

Passaggio 4 Selezionare il servizio di Visual Voicemail creato, quindi selezionare **Avanti** > **Sottoscrivi**.

Impostazione di Visual Voicemail per un gruppo di utenti

Per aggiungere un gruppo di telefoni IP Cisco a Cisco Unified Communications Manager con iscrizione a Visual Voicemail, creare un modello del telefono nello strumento BAT per ciascun tipo di telefono e in ciascun modello del telefono. È possibile quindi effettuare l'iscrizione al servizio Visual Voicemail e utilizzare il modello per inserire i telefoni.

Se i telefoni IP Cisco sono già stati registrati e si desidera effettuare la sottoscrizione al servizio Visual Voicemail, creare un modello telefono nello strumento BAT, effettuare la sottoscrizione al servizio Visual Voicemail nel modello e aggiornare i telefoni tramite lo strumento BAT.

Per ulteriori informazioni, consultare http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html.

AS-SIP (Assured Services SIP)

AS-SIP (Assured Services SIP) è un insieme di funzioni e protocolli che garantiscono un flusso di chiamate estremamente sicuro per i telefoni IP Cisco e i telefoni di terze parti. Le seguenti funzioni sono nell'insieme note come AS-SIP:

- MLPP (Multilevel Precedence and Preemption, Precedenza e prelazione multilivello)
- DSCP (Differentiated Services Code Point)

- TLS (Transport Layer Security) e SRTP (Secure Real-time Transport Protocol)
- IPv6 (protocollo Internet versione 6)

AS-SIP viene spesso utilizzato con MLPP per definire la priorità delle chiamate durante un'emergenza. Con MLPP è possibile assegnare un livello di priorità alle chiamate in uscita, dal livello 1 (più bassa) a 5 (più alta). Quando si riceve una chiamata, sul telefono viene visualizzata un'icona del livello di precedenza che indica la priorità della chiamata.

Per configurare AS-SIP, completare le seguenti operazioni in Cisco Unified Communications Manager:

- Configurare un utente digest: configurare l'utente finale per utilizzare l'autenticazione del digest per le richieste SIP.
- Configurare la porta protetta del telefono SIP: Cisco Unified Communications Manager utilizza questa porta per ascoltare i telefoni per le registrazioni di linea SIP su TLS.
- Riavviare i servizi: dopo aver configurato la porta protetta, riavviare i servizi Cisco Unified Communications Manager e Cisco CTL Provider. Configurare il profilo SIP per AS-SIP: configurare un profilo SIP con impostazioni SIP per gli endpoint AS-SIP e per i trunk SIP. I parametri specifici del telefono non vengono scaricati su un telefono AS-SIP di terze parti. Vengono utilizzati solo da Cisco Unified Manager. I telefoni di terze parti devono configurare localmente le stesse impostazioni.
- Configurare il profilo di protezione del telefono per AS-SIP: è possibile utilizzare il profilo di protezione del telefono per assegnare le impostazioni di protezione quali TLS, SRTP e autenticazione del digest.
- Configurare l'endpoint AS-SIP: configurare un telefono IP Cisco o un endpoint di terze parti con il supporto AS-SIP.
- Associare un dispositivo all'utilizzo finale: associare l'endpoint a un utente.
- Configurazione il profilo di protezione del trunk SIP per AS-SIP: è possibile utilizzare il profilo di protezione del trunk SIP per assegnare a un trunk SIP le funzioni di protezione quali TLS o autenticazione del digest.
- Configurare il trunk SIP per AS-SIP: configurare un trunk SIP con il supporto AS-SIP.
- Configurare le funzioni AS-SIP: configurare ulteriori funzioni AS-SIP come MLPP, TLS, V.150 e IPv6.

Per informazioni dettagliate sulla configurazione di SP-SIP, vedere il capitolo "Configurazione di endpoint As-SIP" nella *Guida alla configurazione del sistema per Cisco Unified Communications Manager*.

Migrazione diretta del telefono a un telefono multipiattaforma

È possibile eseguire facilmente la migrazione del proprio aziendale telefono a un telefono multipiattaforma in un passaggio senza utilizzare il caricamento del firmware di transizione. È sufficiente ottenere e autorizzare la licenza di migrazione dal server.

Per ulteriori informazioni, consultare https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Precedenza e prelazione multilivello

MLPP consente di definire la priorità delle chiamate durante le emergenze o altre situazioni critiche. È possibile assegnare una priorità da 1 a 5 alle chiamate in uscita. Le chiamate in ingresso visualizzano un'icona che

indica la priorità della chiamata. Gli utenti autenticati possono dare la precedenza alle chiamate su determinate stazioni o tramite trunk TDM.

Questa funzionalità assicura valutazione elevato personale di comunicazione per le organizzazioni a critiche e del personale.

MLPP viene spesso utilizzato con AS-SIP (Assured Services SIP). Per informazioni dettagliate sulla configurazione MLPP, vedere il capitolo "Configurazione della precedenza e della prelazione multilivello" nella *Guida alla configurazione del sistema per Cisco Unified Communications Manager*.

Impostazione del Modello softkey

Tramite Cisco Unified Communications Manager Administration, è possibile associare fino a 18 softkey alle applicazioni supportate dal telefono. Cisco Unified Communications Manager supporta il modello di softkey utente standard e funzione standard.

Un'applicazione che supporta le softkey può avere uno o più modelli di softkey standard associati. È possibile modificare un modello di softkey standard facendone una copia, rinominandolo e aggiornando il nuovo modello. È inoltre possibile modificare un modello di softkey non standard.

Il parametro Controllo softkey mostra se le softkey di un telefono sono controllate dalla a funzione Modello softkey. Il parametro Controllo softkey è un campo obbligatorio.

Per ulteriori informazioni sulla configurazione di questa funzione, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

I telefoni IP Cisco non supportano tutte le softkey configurabili in Configurazione modello softkey in Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager consente di abilitare o disabilitare alcune softkey nelle impostazioni di configurazione della regola di controllo. Nella tabella seguente vengono elencate le funzioni e le softkey che è possibile configurare su un modello di softkey e ne viene specificato il supporto sul telefono IP Cisco.

Nota Cisco Unified Communications Manager consente di configurare qualsiasi softkey in un modello di softkey, ma i softkey non supportati non vengono visualizzati sul telefono.

Tabella 38: Softkey configurabili

Funzione	Softkey configurabili nella configurazione Modello softkey	Supportata come softkey
Rispondi	Rispondi (Rispondi)	Supportato
Prenotazione di chiamata	Prenotazione di chiamata (Prenota)	Supportato
Inoltro di tutte le chiamate	Devia tutte (DevTutt)	Supportato
Parcheggio chiamata	Parcheggio chiamata (ParchegChiam)	Supportato
Risposta per assente	Risposta per assente (RispAss)	Supportato
Inclusione	Inclusione	Supportato

Funzione	Softkey configurabili nella configurazione Modello softkey	Supportata come softkey
InclusConf	Inclusione conferenza	Supportato
Conferenza	Conferenza (Conf)	Supportato
Elenco partecipanti conferenza	Elenco partecipanti conferenza (El.Conf.)	Supportato
Devia	Deviazione immediata (ImmDev)	Supportato
Non disturbare	Toggle Do Not Disturb (NoDist)	Supportato
Termina	Termina (Termina)	Supportato
Risposta per assente di gruppo	Risposta per assente di gruppo (RispAsG)	Supportato
Attesa	Attesa (Attesa)	Supportato
Gruppo di ricerca	GrpLog (GrpLog)	Supportato
Collega	Collega (Collega)	Non supportato
Identificazione chiamata indesiderata	Attiva/disattiva Identificazione telefonate indesiderate (ID_TI)	Supportato
Conferenza automatica	Conferenza automatica (ConfAut)	Supportato
Connessione mobile	Mobilità interni telefonici (Mobilità)	Supportato
Nuova chiamata	Nuova chiamata (NvChiam)	Supportato
Risposta per altri gruppi	Risposta per altri gruppi (RispAlG)	Supportato
Supporto PLK per Statistiche coda	Stato coda	Non supportato
Quality Reporting Tool	Quality Reporting Tool (QRT)	Supportato
Ripeti	Ripeti (Ripeti)	Supportato
Rimozione dell'ultimo partecipante alla conferenza	Rimozione dell'ultimo partecipante alla conferenza (Rimuovi)	Non supportato
Riprendi	Riprendi (Ripr.)	Supportato
Seleziona	Seleziona (Selez.)	Non supportato
Chiamata rapida	Composizione abbreviata (ChAbbr)	Supportato
Trasferisci	Trasferisci (Trfr)	Supportato
Comando Modalità video	Comando Modalità video (ModifVis)	Non supportato

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare una delle finestre seguenti:

- Per configurare i modelli di softkey, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Modello softkey**.
- Per assegnare un modello di softkey a un telefono, selezionare **Dispositivo** > **Telefono** e configurare il campo Modello softkey.

Passaggio 2 Salvare le modifiche.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Modelli dei pulsanti del telefono

Tramite i modelli dei pulsanti del telefono, è possibile assegnare le funzioni delle chiamate rapide e di gestione delle chiamate a dei pulsanti programmabili. Le funzioni di gestione delle chiamate che è possibile assegnare ai pulsanti includono Rispondi, Mobilità e Tutte le chiamate.

Come procedura ottimale, modificare i modelli prima di registrare i telefoni sulla rete. In questo modo, sarà possibile accedere alle opzioni personalizzate del modello dei pulsanti del telefono da Cisco Unified Communications Manager durante la registrazione.

Modifica del modello pulsanti del telefono

Per ulteriori informazioni sui servizi del telefono IP e sulla configurazione dei pulsanti linea, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Modello pulsanti telefono**.

Passaggio 2 Fare clic su **Trova**.

Passaggio 3 Selezionare il modello del telefono.

Passaggio 4 Selezionare **Copia**, immettere un nome per il nuovo modello, quindi selezionare **Salva**.

Viene visualizzata la finestra Configurazione modello pulsanti telefono.

Passaggio 5 Individuare il pulsante che si desidera assegnare, quindi selezionare **URL del servizio** dall'elenco a discesa Funzioni associato alla linea.

Passaggio 6 Selezionare **Salva** per creare un nuovo modello dei pulsanti del telefono in cui venga utilizzato l'URL del servizio.

Passaggio 7 Selezionare **Dispositivo** > **Telefono** e aprire la finestra Configurazione telefono relativa al telefono in uso.

Passaggio 8 Selezionare il nuovo modello dei pulsanti del telefono dal relativo elenco a discesa.

Passaggio 9 Selezionare **Salva** per memorizzare la modifica, quindi selezionare **Applica configurazione** per implementare la modifica.

Gli utenti del telefono possono adesso accedere al portale Self Care e associare il servizio a un pulsante del telefono.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Assegnazione del modello pulsanti del telefono per tutte le chiamate

Assegnare un pulsante Tutte le chiamate nel modello telefono per gli utenti con più linee condivise.

Se sul telefono è configurato il pulsante Tutte le chiamate, gli utenti lo utilizzano per:

- Visualizzare un elenco consolidato delle chiamate in corso da tutte le linee del telefono.
- Visualizzare (in Cronologia chiamate) un elenco di tutte le chiamate perse da tutte le linee del telefono.
- Effettuare una chiamata sulla linea principale dell'utente quando l'utente blocca la linea. La funzione Tutte le chiamate torna per impostazione predefinita alla linea principale dell'utente per le chiamate in uscita.

Procedura

Passaggio 1 Modificare il modello dei pulsanti del telefono per includere il pulsante Tutte le chiamate.

Passaggio 2 Assegnare il modello al telefono.

Impostazione della rubrica personale o della funzione Chiamata rapida come servizio del telefono IP

È possibile modificare un modello dei pulsanti del telefono per associare un URL del servizio a un pulsante programmabile. In questo modo, gli utenti disporranno dell'accesso tramite un singolo pulsante alla rubrica personale e alla funzione Chiamate rapide. Prima di modificare il modello dei pulsanti del telefono, è necessario configurare la rubrica personale o la funzione Chiamate rapide come servizi del telefono IP. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Per configurare la rubrica personale o la funzione Chiamata rapida come servizi del telefono IP (se non è già stato fatto), attenersi alla seguente procedura:

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Servizi telefonici**.

Viene visualizzata la finestra Cerca ed elenca servizi telefono IP.

Passaggio 2 Fare clic su **Aggiungi nuovo**.

Viene visualizzata la finestra Configurazione servizi telefono IP.

Passaggio 3 Immettere le seguenti impostazioni:

- Nome servizio: immettere **Rubrica personale**.
- Descrizione servizio: immettere una descrizione facoltativa del servizio.
- URL del servizio

  Per la rubrica personale, immettere l'URL seguente:

  http://<Unified CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  Per la funzione Chiamata rapida, immettere l'URL seguente:

  http://<Unified-CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- URL servizi protetti

  Per la rubrica personale, immettere l'URL seguente:

  https://<Unified CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  Per la funzione Chiamata rapida, immettere l'URL seguente:

  https://<Unified-CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Categoria servizio: selezionare **Servizio XML**.
- Tipo di servizio: selezionare **Rubriche**.
- Abilita: selezionare la casella di controllo.

  http://<IP_address> o *https://<IP_address>* (in base al protocollo supportato dal telefono IP Cisco.)

Passaggio 4 Selezionare **Salva**.

Nota Se l'URL dei servizi viene modificato, se viene rimosso un parametro del servizio del telefono IP o se viene modificato il nome di un parametro di un servizio telefonico a cui gli utenti sono iscritti, è necessario fare clic su **Aggiorna iscrizioni** per aggiornare tutti gli utenti attualmente iscritti e applicare le modifiche apportate; altrimenti, gli utenti dovranno ripetere l'iscrizione al servizio per ricostruire l'URL corretto.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Modifica del modello pulsanti del telefono per la rubrica personale o la composizione veloce

È possibile modificare un modello dei pulsanti del telefono per associare un URL del servizio a un pulsante programmabile. In questo modo, gli utenti disporranno dell'accesso tramite un singolo pulsante alla rubrica personale e alla funzione Chiamate rapide. Prima di modificare il modello dei pulsanti del telefono, è necessario configurare la rubrica personale o la funzione Chiamate rapide come servizi del telefono IP.

Per ulteriori informazioni sui servizi del telefono IP e sulla configurazione dei pulsanti linea, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Impostazioni dispositivo** > **Modello pulsanti telefono**.

Passaggio 2 Fare clic su **Trova**.

Passaggio 3 Selezionare il modello del telefono.

Passaggio 4 Selezionare **Copia**, immettere un nome per il nuovo modello, quindi selezionare **Salva**.

Viene visualizzata la finestra Configurazione modello pulsanti telefono.

Passaggio 5 Individuare il pulsante che si desidera assegnare, quindi selezionare **URL del servizio** dall'elenco a discesa Funzioni associato alla linea.

Passaggio 6 Selezionare **Salva** per creare un nuovo modello dei pulsanti del telefono in cui venga utilizzato l'URL del servizio.

Passaggio 7 Selezionare **Dispositivo** > **Telefono** e aprire la finestra Configurazione telefono relativa al telefono in uso.

Passaggio 8 Selezionare il nuovo modello dei pulsanti del telefono dal relativo elenco a discesa.

Passaggio 9 Selezionare **Salva** per memorizzare la modifica, quindi selezionare **Applica configurazione** per implementare la modifica.

Gli utenti del telefono possono adesso accedere al portale Self Care e associare il servizio a un pulsante del telefono.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Configurazione VPN

La funzione VPN di Cisco consente di mantenere la protezione della rete fornendo al contempo agli utenti un metodo sicuro e affidabile per la connessione alla rete aziendale. Utilizzare questa funzione quando:

- Un telefono si trova all'esterno di una rete attendibile
- Il traffico di rete tra il telefono e Cisco Unified Communications Manager incrocia una rete non attendibile

Sono disponibili tre approcci comuni per l'autenticazione client con una VPN:

- Certificati digitali
- Password
- Nome utente e password

Ciascun metodo presenta dei vantaggi. Tuttavia, se i criteri di sicurezza aziendali lo consentono, si consiglia di scegliere un approccio basato sul certificato poiché i certificati consentono l'accesso continuo senza nessun intervento da parte dell'utente. Sono supportati i certificati LSC e MIC.

Per configurare le funzioni VPN, effettuare innanzitutto il provisioning del dispositivo in sede e distribuire quindi il dispositivo fuori sede.

Per ulteriori informazioni sull'autenticazione del certificato e sull'uso della rete VPN, consultare la Nota tecnica *Telefono VPN AnyConnect con autenticazione del certificato su un esempio di configurazione ASA*. Il documento è disponibile all'URL http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html.

Se si sceglie l'approccio tramite password o nome utente e password, all'utente vengono richieste le credenziali di accesso. Impostare le credenziali di accesso seguendo i requisiti dei criteri di sicurezza aziendali. È inoltre possibile configurare l'impostazione Abilita salvataggio permanente password per salvare la password dell'utente sul telefono. La password dell'utente viene salvata finché non si verifica un tentativo di accesso non riuscito, un utente cancella manualmente la password, il telefono si reimposta o l'alimentazione viene interrotta.

Un altro strumento utile è l'impostazione Abilita rilevazione automatica rete. Quando si abilita questa casella di controllo, il client VPN può essere eseguito soltanto quando rileva di trovarsi al di fuori della rete aziendale. Questa impostazione è disabilitata per impostazione predefinita.

Il telefono di Cisco supporta Cisco SVC IPPhone Client v1.0 come tipo di client.

Per ulteriori informazioni su mantenimento, configurazione e funzionamento di una rete privata virtuale con una VPN, consultare il capitolo "Impostazione della Rete privata virtuale" della *Guida alla protezione per Cisco Unified Communications Manager*. Questo documento è disponibile all'URL http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Per il mantenimento della protezione della rete, la funzione VPN di Cisco utilizza il Secure Sockets Layer (SSL).

Nota Attivare l'impostazione Server TFTP alternativo durante la configurazione di un telefono off-premise per fare in modo che nella VPN con SSL su ASA venga utilizzato un client integrato.

Impostazione di tasti di linea aggiuntivi

Abilitare la modalità di linea avanzata per utilizzare come tasti linea i pulsanti che si trovano su entrambi i lati dello schermo del telefono. In modalità linea avanzata, la composizione predittiva e gli avvisi di chiamata in entrata eseguibili sono abilitati per impostazione predefinita.

Prima di iniziare

È necessario creare un nuovo modello dei pulsanti del telefono.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Individuare il telefono da impostare.

Passaggio 3 Accedere all'area Configurazione specifica del prodotto e impostare il campo **Modalità linea** su **Modalità linea avanzata**.

Passaggio 4 Accedere all'area Informazioni dispositivo e impostare il campo **Modello pulsanti telefono** su un modello personalizzato.

Passaggio 5 Selezionare **Applica configurazione**.

Passaggio 6 Selezionare **Salva**.

Passaggio 7 Riavviare il telefono.

Argomenti correlati

Ambiente in modalità linea sessione, a pagina 168

Funzioni disponibili in modalità linea avanzata

È possibile utilizzare la modalità linea avanzata con Mobile and Remote Access Through Expressway.

Può inoltre essere utilizzata con una linea di rollover, una configurazione di instradamento delle chiamate in cui le chiamate vengono inoltrate a un'altra linea condivisa se la linea condivisa iniziale è occupata. Quando la modalità di linea avanzata viene utilizzata con una linea di rollover, le chiamate recenti a linee condivise vengono consolidate in un unico numero della rubrica. Per ulteriori informazioni sulle linee di rollover, consultare *Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager* per Cisco Unified Communications Manager 12.0 (1) o versioni successive.

La modalità di linea avanzata supporta la maggior parte delle funzionalità, ma non tutte. L'abilitazione di funzione non implica il supporto. Per sapere se una funzione è supportata, fare riferimento alla tabella seguente.

Tabella 39: Supporto funzioni e modalità linea avanzata

Funzione	Supportato	Versione del firmware
Rispondi	Sì	11.5(1) e successive
Risposta automatica alle chiamate	Sì	11.5(1) e successive
Inclusione/InclusConf	Sì	11.5(1) e successive
Parcheggio chiamata indirizzato con indicatore di stato	Sì	12.0(1) e successive
Integrazione smartphone Bluetooth	No	-
Cuffie USB Bluetooth	Sì	11.5(1) e successive
Prenotazione di chiamata	Sì	11.5(1) e successive
Call Chaperone	No	-
Inoltro di tutte le chiamate	Sì	11.5(1) e successive
Parcheggio chiamata	Sì	12.0(1) e successive
Stato linea Parcheggio chiamata	Sì	12.0(1) e successive
Risposta per assente	Sì	11.5(1) e successive
Stato linea Risposta per Assente	Sì	11.5(1) e successive
Inoltro di tutte le chiamate su più linee	Sì	11.5(1) e successive

Funzione	Supportato	Versione del firmware
Cisco Extension Mobility Cross Cluster	Sì	La versione 12.0 (1) e successive supporta questa funzione.
Cisco IP Manager Assistant (IPMA)	No	-
Cisco Unified Communications Manager Express	No	-
Conferenza	Sì	11.5(1) e successive
Applicazioni CTI (Computer Telephony Integration)	Sì	11.5(1) e successive
Rifiuta	Sì	11.5(1) e successive
Registrazione richiesta dal dispositivo	Sì	11.5(1)SR1 e successive
Non disturbare	Sì	11.5(1) e successive
SRST migliorata	No	-
Extension Mobility	Sì	11.5(1) e successive
Risposta per assente di gruppo	Sì	La versione 12.0 (1) e successive supporta questa funzione.
Attesa	Sì	11.5(1) e successive
Gruppi di ricerca	Sì.	12.0(1) e successive
Avviso di chiamata in arrivo con timer configurabile	No	-
Interfono	Sì	11.5(1) e successive
modulo di espansione chiave	Il modulo di espansione tasti del telefono IP Cisco 8851/8861 e il modulo di espansione tasti del telefono IP Cisco 8865 supportano la modalità linea avanzata	12.0(1) e successive
Identificazione telefonate indesiderate (ID_TI)	Sì	11.5(1) e successive
Conferenza automatica	Sì	11.5(1) e successive
Connessione mobile	Sì	11.5(1) e successive
Precedenza e prelazione multilivello	No	-

Funzione	Supportato	Versione del firmware
Disattiva audio	Sì	11.5(1) e successive
Risposta per altri gruppi	Sì	12.0(1) e successive
Supporto PLK (Programmable Line Key) per Stato coda	Sì	11.5(1) e successive
Privacy	Sì	11.5(1) e successive
Stato coda	Sì	11.5(1) e successive
Quality Reporting Tool (QRT)	Sì	11.5(1) e successive
Supporto impostazioni internazionali con scrittura da destra verso sinistra	No	-
Ripeti	Sì	11.5(1) e successive
Monitoraggio e registrazione silenziosi	Sì	11.5(1)SR1 e successive
Chiamata rapida	Sì	11.5(1) e successive
Survivable Remote Site Telephony (SRST)	Sì	11.5(1) e successive
Trasferisci	Sì	11.5(1) e successive
Composizione URI (Uniform Resource Identifier)	Sì	11.5(1) e successive
Videochiamate	Sì	11.5(1) e successive
Segreteria telefonica visiva	Sì	11.5(1) e successive
Casella vocale	Sì	11.5(1) e successive

Argomenti correlati

Ambiente in modalità linea sessione, a pagina 168

Impostazione del timer di riavvio TLS

Il riavvio della sessione TLS consente di riprendere una sessione TLS senza dover ripetere l'intero processo di autenticazione TLS. In questo modo, è possibile ridurre notevolmente il tempo necessario per lo scambio dei dati da parte della connessione TLS.

Anche se i telefoni supportano le sessioni TLS, le sessioni TLS non supportano il riavvio TLS. Nell'elenco seguente viene descritto il supporto delle diverse sessioni e del riavvio TLS:

- Sessione TLS per segnalazione SIP: riavvio supportato

- Client HTTPS: riavvio supportato
- CAPF: riavvio supportato
- TVS: riavvio supportato
- EAP-TLS: riavvio non supportato
- EAP-FAST: riavvio non supportato
- Client VPN: riavvio non supportato

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Impostare il parametro del timer di riavvio TLS.

L'intervallo per il timer è compreso tra 0 e 3600 secondi. Il valore predefinito è 3600. Se questo campo è impostato su 0, il riavvio della sessione TLS è disabilitato.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Abilitazione di Intelligent Proximity

Nota Questa procedura si applica esclusivamente ai telefoni abilitati per il Bluetooth. I telefoni IP Cisco 8811, 8841, 8851NR e 8865NR non supportano il Bluetooth.

Intelligent Proximity consente agli utenti di trarre il massimo dalle proprietà acustiche del telefono utilizzando il proprio dispositivo mobile o tablet. L'utente associa il dispositivo mobile o il tablet al telefono tramite Bluetooth.

In seguito all'associazione del dispositivo mobile, l'utente può quindi effettuare e ricevere sul telefono le chiamate al cellulare. Con un tablet, l'utente può indirizzare l'audio dal tablet al telefono.

Gli utenti possono abbinare più dispositivi mobili, tablet e cuffie Bluetooth al telefono. Tuttavia, è possibile connettere contemporaneamente solo un dispositivo e una cuffia.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare **Telefono** > **Dispositivo**.

Passaggio 2 Individuare il telefono che si desidera modificare.

Passaggio 3 Individuare il campo Bluetooth e impostarlo su **Abilitato**.

Passaggio 4 Individuare il campo Consenti modalità Vivavoce mobile Bluetooth e impostarlo su **Abilitato**.

Passaggio 5 Salvare le modifiche e applicarle al telefono.

Impostazione della risoluzione di trasmissione del video

I telefoni IP Cisco 8845, 8865 e 8865NR supportano i formati video seguenti:

- 720p (1280 x 720)
- WVGA (800 x 480)
- 360p (640 x 360)
- 240p (432 x 240)
- VGA (640 x 480)
- CIF (352 x 288)
- SIF (352 x 240)
- QCIF (176 x 144)

I telefoni IP Cisco con capacità video negoziano la risoluzione migliore per la larghezza di banda in base alle configurazioni o alle limitazioni di risoluzione del telefono. Esempio: su una chiamata 88 x 5 per 88 x 5 diretta, i telefoni non inviano 720p reali, ma 800 x 480. Questa limitazione è dovuta alla risoluzione di 800 x 480 dello schermo WVGA di 5" sulla chiamata 88 x 5.

Tipo di video	Risoluzione video	Fotogrammi al secondo (fps)	Intervallo velocità in bit video
720p	1280 x 720	30	1360-2500 kbps
720p	1280 x 720	15	790-1359 kbps
WVGA	800 x 480	30	660-789 kbps
WVGA	800 x 480	15	350-399 kbps
360p	640 x 360	30	400-659 kbps
360p	640 x 360	15	210–349 kbps
240p	432 x 240	30	180–209 kbps
240p	432 x 240	15	64–179 kbps
VGA	640 x 480	30	520–1500 kbps
VGA	640 x 480	15	280–519 kbps
CIF	352 x 288	30	200-279 kbps
CIF	352 x 288	15	120-199 kbps

Tipo di video	Risoluzione video	Fotogrammi al secondo (fps)	Intervallo velocità in bit video
SIF	352 x 240	30	200-279 kbps
SIF	352 x 240	15	120-199 kbps
QCIF	176 x 144	30	94-119 kbps
QCIF	176 x 144	15	64-93 kbps

Gestione delle cuffie sulle versioni precedenti di Cisco Unified Communications Manager

Se si dispone di una versione di Cisco Unified Communications Manager precedente alla 12.5(1)SU1, è possibile configurare in remoto le impostazioni della cuffia Cisco per l'uso con i telefoni in sede.

Per configurare la cuffia remota in Cisco Unified Communications Manager 10.5(2), 11.0(1), 11.5(1), 12.0(1) e 12.5(1), è necessario scaricare un file dal sito Web di download del software Cisco, modificarlo e caricarlo sul server TFTP di Cisco Unified Communications Manager. Il file è un file JSON (JavaScript Object Notification). La configurazione della cuffia aggiornata viene applicata alle cuffie aziendali in un intervallo di tempo da 10 a 30 minuti per impedire il backlog di traffico sul server TFTP.

Nota È possibile gestire e configurare le cuffie tramite Cisco Unified Communications Manager Administration versione 11.5(1)SU7.

Tenere presente quanto segue quando si lavora con il file JSON:

- Le impostazioni non vengono applicate se nel codice mancano una o più parentesi. Utilizzare uno strumento online, ad esempio JSON Formatter, e verificare il formato.
- Impostare "**updatedTime**" sull'ora corrente, altrimenti la configurazione non viene applicata. In alternativa, è possibile aumentare il valore **updatedTime** di 1 per renderlo più grande della versione precedente.
- Non modificare il nome del parametro, altrimenti l'impostazione non verrà applicata.

Per ulteriori informazioni sul servizio TFTP, vedere il capitolo "Gestione del firmware del dispositivo" nella *Guida all'amministrazione di Cisco Unified Communications Manager e IM and Presence Service*.

Prima di applicare il file `defaultheadsetconfig.json`, eseguire l'aggiornamento alla versione più recente del firmware del telefono. Nella tabella riportata di seguito vengono descritte le impostazioni predefinite che è possibile regolare con il file JSON.

Download del file di configurazione della cuffia predefinito

Prima di configurare i parametri delle cuffie in remoto, è necessario scaricare il file di esempio JSON (JavaScript Object Notation) più recente.

Procedura

Passaggio 1 Accedere al seguente URL: https://software.cisco.com/download/home/286320550.

Passaggio 2 Scegliere **Cuffie Cisco serie 500**.

Passaggio 3 Selezionare la serie della cuffia.

Passaggio 4 Scegliere la cartella di una versione e selezionare il file zip.

Passaggio 5 Fare clic sul pulsante **Scarica** o **Aggiungi al carrello** e seguire le istruzioni.

Passaggio 6 Decomprimere il file zip in una directory del PC.

Operazioni successive

Modifica del file di configurazione della cuffia predefinito, a pagina 211

Modifica del file di configurazione della cuffia predefinito

Se si utilizza il file JSON (JavaScript Object Notation), tenere presente quanto segue:

- Le impostazioni non vengono applicate se nel codice mancano una o più parentesi. Utilizzare uno strumento online, ad esempio JSON Formatter, e verificare il formato.
- Impostare "**updatedTime**" sull'ora corrente, altrimenti la configurazione non viene applicata.
- Confermare che **firmwareName** è `LATEST` (più recente) altrimenti le configurazioni non verranno applicate.
- Non modificare un nome di parametro, altrimenti l'impostazione non verrà applicata.

Procedura

Passaggio 1 Aprire il file `defaultheadsetconfig.json` con un editor di testo.

Passaggio 2 Modificare i valori del parametro **updatedTime** e della cuffia che si desidera modificare.

Di seguito è riportato uno script di esempio. Lo script viene fornito soltanto come riferimento. Utilizzarlo come guida per configurare i parametri della cuffia. Utilizzare il file JSON incluso nel caricamento del firmware.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
```

```
  ],
  "modelFirmware": [
    {
      "firmwareName": "LATEST",
      "latest": true,
      "firmwareParams": [
        {
          "name": "Speaker Volume",
          "access": "Both",
          "usageId": 32,
          "value": 7
        },
        {
          "name": "Microphone Gain",
          "access": "Both",
          "usageId": 33,
          "value": 2
        },
        {
          "name": "Sidetone",
          "access": "Both",
          "usageId": 34,
          "value": 1
        },
        {
          "name": "Equalizer",
          "access": "Both",
          "usageId": 35,
          "value": 3
        }
      ]
    }
  ]
},
{
  "modelSeries": "560",
  "models": [
    "560",
    "561",
    "562"
  ],
  "modelFirmware": [
    {
      "firmwareName": "LATEST",
      "latest": true,
      "firmwareParams": [
        {
          "name": "Speaker Volume",
          "access": "Both",
          "usageId": 32,
          "value": 7
        },
        {
          "name": "Microphone Gain",
          "access": "Both",
          "usageId": 33,
          "value": 2
        },
        {
          "name": "Sidetone",
          "access": "Both",
          "usageId": 34,
          "value": 1
        },
```

```
                    {
                      "name": "Equalizer",
                      "access": "Both",
                      "usageId": 35,
                      "value": 3
                    },
                    {
                      "name": "Audio Bandwidth",
                      "access": "Admin",
                      "usageId": 36,
                      "value": 0
                    },
                    {
                      "name": "Bluetooth",
                      "access": "Admin",
                      "usageId": 39,
                      "value": 0
                    },
                    {
                      "name": "DECT Radio Range",
                      "access": "Admin",
                      "usageId": 37,
                      "value": 0
                    }
                    {
                       "name": "Conference",
                      "access": "Admin",
                      "usageId": 41,
                      "value": 0
                  ]
                }
              ]
            }
          ]
        }
      }
}
```

Passaggio 3 Salvare il file `defaultheadsetconfig.json`.

Operazioni successive

Installare il file di configurazione predefinito.

Installazione del file di configurazione predefinito in Cisco Unified Communications Manager

Dopo aver modificato il file `defaultheadsetconfig.json`, installarlo su Cisco Unified Communications Manager utilizzando lo strumento di gestione dei file TFTP.

Procedura

Passaggio 1 In Cisco Unified OS Administration, selezionare **Aggiornamenti software** > **Gestione file TFTP**.

Passaggio 2 Selezionare **Carica file**.

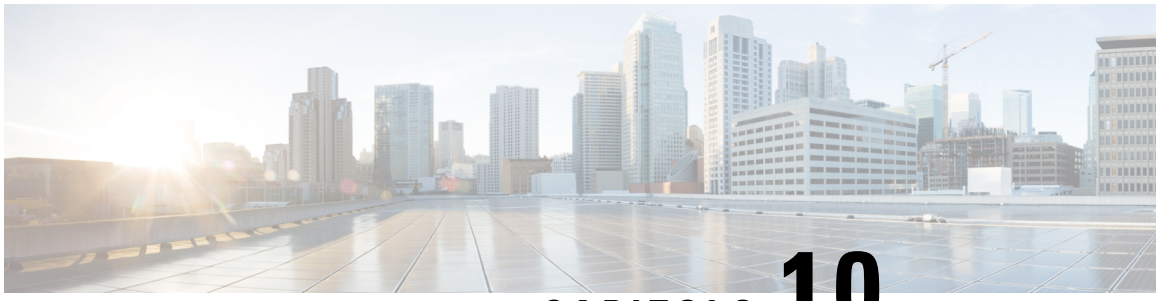
Passaggio 3	Selezionare **Scegli file** e passare al file `defaultheadsetconfig.json`.
Passaggio 4	Selezionare **Carica file**.
Passaggio 5	Fare clic su **Chiudi**.

Riavvio del server TFTP Cisco

Dopo aver caricato il file `defaultheadsetconfig.json` nella directory TFTP, riavviare il server TFTP di Cisco e reimpostare i telefoni. Dopo circa 10-15 minuti, inizia la procedura di download e le nuove configurazioni vengono applicate alle cuffie. L'applicazione delle impostazioni richiede da 10 a 30 minuti.

Procedura

Passaggio 1	Eseguire l'accesso a Cisco Unified Serviceability e scegliere **Tools** > **Control Center - Feature Services** (Strumenti > Centro di controllo > Servizi funz.).
Passaggio 2	Dalla casella di riepilogo a discesa **Server**, scegliere il server su cui è in esecuzione il servizio Cisco TFTP.
Passaggio 3	Fare clic sul pulsante di opzione corrispondente al servizio **Cisco TFTP**.
Passaggio 4	Fare clic su **Riavvia**.



CAPITOLO 10

Rubrica aziendale ed Elenco personale

Impostazione della rubrica aziendale

Tramite la rubrica aziendale, l'utente può effettuare la ricerca dei numeri di telefono dei propri colleghi. Per supportare questa funzione, è necessario configurare le rubriche aziendali.

Cisco Unified Communications Manager utilizza una directory LDAP (Lightweight Directory Access Protocol) per memorizzare le informazioni di autenticazione e autorizzazione relative agli utenti delle applicazioni Cisco Unified Communications Manager che si interfacciano con Cisco Unified Communications Manager. In base all'autenticazione vengono determinati i diritti di accesso al sistema da parte degli utenti. L'autorizzazione identifica le risorse di telefonia, come ad esempio un interno specifico, che possono essere utilizzate dagli utenti.

I telefoni IP Cisco utilizzano l'allocazione dinamica per SecureApp su client e server. In questo modo il telefono può leggere i certificati di dimensioni maggiori di 4 KB e riduce la frequenza dei messaggi di errore `Host non trovato` quando un utente accede alla directory.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Al termine della configurazione della rubrica LDAP, gli utenti possono utilizzare il servizio Rubrica aziendale sul telefono per cercare gli altri utenti nella rubrica aziendale.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Impostazione dell'Elenco personale

Tramite l'Elenco personale, l'utente può memorizzare un insieme di numeri personali.

Nell'Elenco personale sono disponibili le funzioni seguenti:

- Rubrica personale (PAB)
- Chiamate rapide

- Address Book Synchronization Tool (TABSynch)

Per accedere alle funzioni dell'Elenco personale, gli utenti possono utilizzare questi metodi:

- Da un browser Web: gli utenti possono accedere alle funzioni Rubrica personale e Chiamata rapida dal portale Self Care di Cisco Unified Communications.
- Dal telefono IP Cisco: selezionare **Contatti** per effettuare una ricerca nella rubrica aziendale o nell'Elenco personale dell'utente.
- Da un'applicazione di Microsoft Windows, gli utenti possono utilizzare lo strumento TABSynch per sincronizzare le proprie rubriche personali con la rubrica di Microsoft Windows (WAB). Se si desidera utilizzare la rubrica di Microsoft Outlook (OAB), è necessario importare i dati dalla rubrica OAB nella rubrica WAB. Solo dopo tale operazione è possibile utilizzare TabSync per sincronizzare la rubrica WAB con l'Elenco personale. Per istruzioni su TABSync, consultare Download del programma di sincronizzazione della rubrica del telefono IP Cisco, a pagina 217 e Impostazione del programma di sincronizzazione, a pagina 218.

I telefoni IP Cisco utilizzano l'allocazione dinamica per SecureApp su client e server. In questo modo il telefono può leggere i certificati di dimensioni maggiori di 4 KB e riduce la frequenza dei messaggi di errore `Host non trovato` quando un utente accede alla directory.

Per assicurarsi che gli utenti del programma di sincronizzazione della rubrica del telefono IP Cisco accedano soltanto ai relativi dati sull'utente finale, attivare Cisco UXL Web Service sin Cisco Unified Serviceability.

Per configurare l'Elenco personale da un browser Web, gli utenti devono effettuare l'accesso al portale Self Care. È necessario fornire agli utenti l'URL e le informazioni di accesso.

Impostazione delle voci dell'Elenco personale dell'utente

Gli utenti possono configurare le voci dell'Elenco personale sul telefono IP Cisco. Per configurare un Elenco personale, gli utenti devono disporre dell'accesso a quanto segue:

- Portale Self Care: assicurarsi che gli utenti conoscano le modalità di accesso al portale Self Care. Per informazioni, vedere Impostazione dell'accesso degli utenti al portale Self Care, a pagina 83.
- Programma di sincronizzazione della rubrica del telefono IP Cisco: assicurarsi di fornire agli utenti il programma di installazione. Consultare Download del programma di sincronizzazione della rubrica del telefono IP Cisco, a pagina 217.

Nota Il programma di sincronizzazione della rubrica del telefono IP Cisco è supportato solo nelle versioni non supportate di Windows (ad esempio, Windows XP e versioni precedenti). Lo strumento non è supportato nelle versioni più recenti di Windows. In futuro, verrà rimosso dall'elenco dei plug-in di Cisco Unified Communications Manager.

Download del programma di sincronizzazione della rubrica del telefono IP Cisco

Per scaricare una copia del programma di sincronizzazione da inviare agli utenti, attenersi alla procedura seguente:

Procedura

Passaggio 1	Per scaricare il programma di installazione, selezionare **Applicazioni** > **Plug-in** da Cisco Unified Communications Manager Administration.
Passaggio 2	Selezionare **Download** accanto al nome del plug-in del programma di sincronizzazione della rubrica del telefono IP Cisco.
Passaggio 3	Quando viene visualizzata la finestra di dialogo per il download del file, selezionare **Salva**.
Passaggio 4	Inviare il file TabSyncInstall.exe e le istruzioni riportate in Distribuzione del programma di sincronizzazione della rubrica del telefono IP Cisco, a pagina 217a tutti gli utenti che necessitano di questa applicazione.

Distribuzione del programma di sincronizzazione della rubrica del telefono IP Cisco

Il programma di sincronizzazione della rubrica del telefono IP Cisco consente di sincronizzare i dati archiviati nella rubrica di Microsoft Windows con la rubrica di Cisco Unified Communications Manager e con la rubrica personale del portale Self Care.

Suggerimento Per sincronizzare correttamente la rubrica di Windows con la rubrica personale, occorre inserire nella rubrica di Windows tutti i relativi utenti prima di effettuare le procedure seguenti.

Installazione del programma di sincronizzazione

Per installare il programma di sincronizzazione della rubrica del telefono IP Cisco, attenersi alla procedura seguente:

Procedura

Passaggio 1	Richiedere all'amministratore del sistema il file di installazione del programma di sincronizzazione della rubrica del telefono IP Cisco.
Passaggio 2	Fare doppio clic sul file TabSyncInstall.exe fornito dall'amministratore.
Passaggio 3	Selezionare **Esegui**.
Passaggio 4	Selezionare **Avanti**.
Passaggio 5	Leggere le informazioni del Contratto di licenza e selezionare **Accetto**. Selezionare **Avanti**.
Passaggio 6	Scegliere la directory in cui installare l'applicazione e selezionare **Avanti**.
Passaggio 7	Selezionare **Installa**.

Passaggio 8 Selezionare **Fine**.

Passaggio 9 Per completare il processo, seguire i passaggi riportati in Impostazione del programma di sincronizzazione, a pagina 218.

Impostazione del programma di sincronizzazione

Per configurare il programma di sincronizzazione della rubrica del telefono IP Cisco, attenersi alla procedura seguente:

Procedura

Passaggio 1 Aprire il programma di sincronizzazione della rubrica del telefono IP Cisco.

Se si è accettata la rubrica di installazione predefinita, è possibile aprire l'applicazione scegliendo **Start** > **Tutti i programmi** > **Cisco Systems** > **TabSync**.

Passaggio 2 Per configurare le informazioni utente, selezionare **Utente**.

Passaggio 3 Immettere il nome utente e la password del telefono IP Cisco e selezionare **OK**.

Passaggio 4 Per configurare le informazioni sul server Cisco Unified Communications Manager, selezionare **Server**.

Passaggio 5 Immettere l'indirizzo IP o il nome host e il numero di porta del server Cisco Unified Communications Manager e selezionare **OK**.

Se non si conoscono queste informazioni, rivolgersi all'amministratore di sistema.

Passaggio 6 Per avviare il processo di sincronizzazione della rubrica, selezionare **Sincronizza**.

La finestra Stato sincronizzazione contiene le informazioni sullo stato della sincronizzazione della rubrica. Se si sceglie l'intervento dell'utente per la regola delle voci duplicate e sono presenti voci di rubrica duplicate, viene visualizzata la finestra Selezione duplicato.

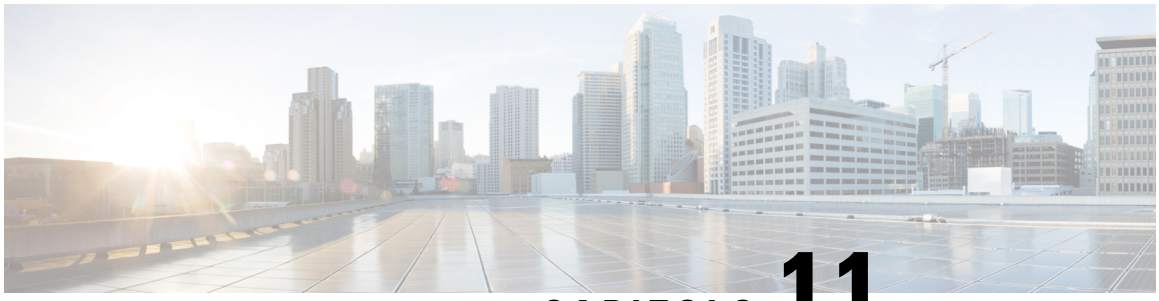
Passaggio 7 Scegliere la voce da includere nella rubrica personale e selezionare **OK**.

Passaggio 8 Al termine della sincronizzazione, selezionare **Esci** per chiudere Cisco Unified CallManager Address Book Synchronizer.

Passaggio 9 Per verificare che la sincronizzazione sia stata completata correttamente, accedere al portale Self Care e selezionare **Rubrica personale**. Dovrebbero venire elencati gli utenti della rubrica di Windows.

PARTE IV

Risoluzione dei problemi del telefono IP Cisco



CAPITOLO 11

Monitoraggio dei sistemi telefonici

Stato del telefono IP Cisco

In questa sezione viene descritto come visualizzare le informazioni sul modello, i messaggi di stato e le statistiche di rete sui telefoni IP Cisco serie 8800.

- Informazioni modello: visualizza le informazioni su hardware e software del telefono.
- Menu Stato: fornisce accesso alle schermate su cui vengono mostrati i messaggi di stato, le statistiche di rete e le statistiche per la chiamata in corso.

È possibile utilizzare le informazioni visualizzate in queste schermate per monitorare il funzionamento di un telefono e per assistenza durante la risoluzione dei problemi.

È inoltre possibile ottenere molte di tali informazioni e altri dati correlati da remoto tramite la pagina Web del telefono.

Per ulteriori informazioni sulla risoluzione dei problemi, consultare Risoluzione dei problemi, a pagina 257.

Visualizzazione della finestra Informazioni telefono

Per visualizzare la schermata Informazioni modello, attenersi alla procedura seguente.

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Informazioni telefono**.

Se l'utente è collegato a un server sicuro o autenticato, viene visualizzata l'icona corrispondente (blocco o certificato) nella schermata Informazioni telefono a destra dell'opzione del server. Se l'utente non è collegato a un server sicuro o autenticato, non viene visualizzata alcuna icona.

Passaggio 3 Per uscire dalla schermata Informazioni modello, premere **Esci**.

Campi di Informazioni telefono

Nella tabella seguente vengono descritte le impostazioni di Informazioni telefono.

Tabella 40: Impostazioni di Informazioni telefono

Opzione	Descrizione
Numero modello	Numero di modello del telefono.
Indirizzo IPv4	Indirizzo IP del telefono.
Nome host	Nome host del telefono.
Carico attivo	Versione del firmware attualmente installata sul telefono. L'utente può premere **Dettagli** per ulteriori informazioni.
Carico inattivo	Il carico inattivo viene visualizzato soltanto mentre è in corso un download. Vengono visualizzati anche un'icona di download e uno stato di «Aggiornamento in corso» o «Aggiornamento non riuscito». Se un utente preme **Dettagli** durante un aggiornamento, vengono elencati il nome file e i componenti del download. È possibile impostare una nuova immagine del firmware per il download anticipato di una finestra di manutenzione. In questo modo, invece di attendere che tutti i telefoni completino il download del firmware, il sistema passa più rapidamente tra la reimpostazione di un carico esistente sullo stato Inattivo e l'installazione di un nuovo carico. Al completamento del download, l'icona cambia per indicare lo stato Completato e viene visualizzato un segno di spunta per indicare la riuscita del download o una «X» per indicare la mancata riuscita del download. Se possibile, il download del resto dei caricamenti prosegue.
Ultimo aggiornamento	Data dell'aggiornamento più recente del firmware.
Server attivo	Nome di dominio del server in cui è stato registrato il telefono.
Server stand-by	Nome di dominio del server di stand-by.

Visualizzazione del menu Stato

Il menu Stato include le opzioni seguenti che forniscono informazioni sul telefono e sul suo funzionamento:

- Messaggi di stato: visualizza la schermata Messaggi di stato in cui è presente un registro dei messaggi di sistema importanti.

- Statistiche Ethernet: visualizza la schermata Statistiche Ethernet in cui sono riportate le statistiche sul traffico Ethernet.
- Statistiche wireless: visualizza la schermata Statistiche wireless, se applicabile.
- Statistiche chiamate: visualizza il numero e le statistiche relativi alla chiamata corrente.
- Punto di accesso attuale: visualizza la schermata Punto di accesso attuale, se applicabile.

Per visualizzare il menu Stato, attenersi alla procedura seguente:

Procedura

Passaggio 1	Per visualizzare il menu Stato, premere **Applicazioni** .
Passaggio 2	Selezionare **Impostazioni amministratore** > **Stato**.
Passaggio 3	Per uscire dal menu Stato, premere **Esci**.

Visualizzazione della finestra Messaggi di stato

La finestra Messaggi di stato visualizza i 30 messaggi di stato più recenti generati dal telefono. È possibile accedere a questa schermata in qualsiasi momento, anche se il telefono non ha completato l'avvio.

Procedura

Passaggio 1	Premere **Applicazioni** .
Passaggio 2	Selezionare **Impostazioni amministratore** > **Stato** > **Messaggi di stato**.
Passaggio 3	Per rimuovere i messaggi di stato correnti, premere **Cancella**.
Passaggio 4	Per uscire dalla schermata Messaggi di stato, premere **Esci**.

Campi di Messaggi di stato

Nella tabella segente vengono descritti i messaggi di stato visualizzati nella schermata Messaggi di stato del telefono.

Tabella 41: Messaggi di stato sul telefono IP Cisco Unified

Messaggio	Descrizione	Spiegazione possibile e azione
Errore dimensione TFTP	Il file di configurazione è troppo grande per il file system del telefono.	Spegnere e riaccendere il telefo
Errore checksum	Il file del software scaricato è danneggiato.	Ottenere una nuova copia del f inserirla nella directory TFTPP questa directory solo quando il chiuso; in caso contrario, i file

Messaggio	Descrizione	Spiegazione possibile e azione
Impossibile acquisire un indirizzo IP da DHCP	Il telefono non ha ricevuto in precedenza un indirizzo IP da un server DHCP. Questo può verificarsi quando si effettua un ripristino delle impostazioni predefinite.	Verificare che siano disponibili il s indirizzo IP per il telefono.
CTL e ITL installati	I file CTL e ITL sono installati nel telefono.	Nessuna. Questo messaggio è solo
CTL installato	Un file CTL (Certificate Trust List) è installato nel telefono.	Nessuna. Questo messaggio è solo non è stato installato in precedenza
Aggiornamento CTL non riuscito	Il telefono non è stato in grado di aggiornare il file CTL (Certificate Trust List).	Problema con il file CTL sul serve
Timeout DHCP	Il server DHCP non ha risposto.	La rete è occupata: gli errori si risc con la riduzione del carico di rete. Nessuna connettività di rete tra il se verificare le connessioni di rete. Il server DHCP è inattivo: controlla server DHCP. Gli errori persistono: provare ad as statico.
Timeout DNS	Il server DNS non ha risposto.	La rete è occupata: gli errori si risc con la riduzione del carico di rete. Nessuna connettività di rete tra il s verificare le connessioni di rete. Il server DNS è inattivo: controllar server DNS.
Host DNS sconosciuto	Il DNS non è in grado di risolvere il nome del server TFTP o di Cisco Unified Communications Manager.	Verificare che i nomi host del serv Unified Communications Manager correttamente nel DNS. Provare a utilizzare gli indirizzi IP
IP duplicato	Un altro dispositivo utilizza l'indirizzo IP assegnato al telefono.	Se il telefono ha un indirizzo IP sta aver assegnato un indirizzo IP dup Se si utilizza DHCP, controllare la c DHCP.
Cancellazione dei file CTL e ITL	Cancellazione del file CTL o ITL.	Nessuna. Questo messaggio è solo

Messaggio	Descrizione	Spiegazione possibile e azione
Errore aggiornamento impostazioni internazionali	Impossibile trovare uno o più file di localizzazione nella directory TFTPPath, oppure i file non sono validi. Le impostazioni internazionali non sono state modificate.	Da Cisco Unified Operating Sy verificare che i file seguenti si secondarie nella gestione dei fi • Ubicato nella directory se delle impostazioni interna • tones.xml • Ubicati nella directory sec delle impostazioni interna • glyphs.xml • dictionary.xml • kate.xml
File non trovato <Cfg File>	Il file di configurazione predefinito e basato sul nome non è stato trovato sul server TFTP.	Il file di configurazione di un t il telefono viene aggiunto al da Communications Manager. Se database di Cisco Unified Com server TFTP genera una rispos **trovato**. • Il telefono non è registrato Communications Manage Occorre aggiungere il tele Unified Communications la registrazione automatic Metodi di aggiunta del tel • Se si utilizza il DHCP, ver punti al server TFTP corr • Se si utilizzano gli indiriz configurazione del server
File non trovato <CTLFile.tlv>	Questo messaggio viene visualizzato sul telefono quando il cluster Cisco Unified Communications Manager non è in modalità protetta.	Nessun impatto, il telefono può Unified Communications Man
Indirizzo IP rilasciato	Il telefono è configurato per rilasciare l'indirizzo IP.	Il telefono rimane in stand-by f riacceso o si reimposta l'indiriz
ITL installato	Il file ITL è installato nel telefono.	Nessuna. Questo messaggio è s non è stato installato in precede

Messaggio	Descrizione	Spiegazione possibile e azione
Caricamento HC non riuscito	L'applicazione scaricata non è compatibile con l'hardware del telefono.	Si verifica se si è tentato di installa software sul telefono che non supp hardware al telefono. Controllare l'ID del carico assegna Unified Communications Manager **Telefono**). Reinserire il carico visu
Nessun router predefinito	DHCP o la configurazione statica non ha specificato alcun router predefinito.	Se il telefono dispone di un indiriz che il router predefinito sia config Se si utilizza il DHCP, il server DH router predefinito. Controllare la c DHCP.
Server DNS non specificato	È stato specificato un nome ma nella configurazione DHCP o dell'IP statico non è stato specificato alcun indirizzo del server DNS.	Se il telefono dispone di un indiriz che il server DNS sia configurato. Se si utilizza il DHCP, il server DH server DNS. Controllare la configur
Nessuna Trust List installata	Il file CTL o il file ITL non è installato nel telefono.	La Trust List non è configurata su Communications Manager, che no per impostazione predefinita.
Impossibile registrare il telefono. La dimensione della chiave del certificato non è conforme a FIPS.	Per FIPS è necessario che la dimensione del certificato del server RSA sia 2048 bit o superiore.	Aggiornare il certificato.
Riavvio richiesto da Cisco Unified Communications Manager	Il telefono si riavvia a causa di una richiesta di Cisco Unified Communications Manager.	Le modifiche alla configurazione s apportate al telefono in Cisco Unif Manager ed è stato premuto Appli
Errore accesso TFTP	Il server TFTP punta a una directory inesistente.	Se si utilizza il DHCP, verificare c al server TFTP corretto. Se si utilizzano indirizzi IP statici, configurazione del server TFTP.
Errore TFTP	Il telefono non riconosce un codice di errore fornito dal server TFTP.	Contattare Cisco TAC (Technical A
Timeout TFTP	Il server TFTP non risponde.	La rete è occupata: gli errori si risc con la riduzione del carico di rete. Nessuna connettività di rete tra il s verificare le connessioni di rete. Il server TFTP è inattivo: controlla server TFTP.
Timeout	Il richiedente ha tentato una transazione 802.1X ma si è verificato un timeout a causa dell'assenza di autenticatore.	In genere, si verifica un timeout de 802.1X non è configurato sullo sw

Messaggio	Descrizione	Spiegazione possibile e azione
Aggiornamento della Trust List non riuscito	Aggiornamento non riuscito dei file CTL e ITL.	Nel telefono sono installati i fi possibile effettuare l'aggiornam Possibili motivi dell'errore: • Si è verificato un guasto d • Il server TFTP non era att • Il nuovo token di sicurezz CTL e il certificato TFTP ITL sono stati introdotti, r file CTL e ITL correnti in • Si è verificato un errore in Soluzioni possibili: • Controllare la connettività • Verificare che il server TF funzionante. • Se il server Transactional supportato in Cisco Unifie verificare che sia attivo e • Verificare che il token di s siano validi. Eliminare manualmente i file C precedenti non sono risultate u
Trust List aggiornata	Il file CTL, il file ITL o entrambi i file sono aggiornati.	Nessuna. Questo messaggio è s
Err. versione	Il nome del file di carico del telefono non è corretto.	Verificare che il file di avvio d corretto.
XmlDefault.cnf.xml o .cnf.xml corrispondente al nome del telefono	Nome del file di configurazione.	Nessuna. Questo messaggio in configurazione del telefono.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Visualizzazione della schermata Informazioni sulla rete

Utilizzare le informazioni visualizzate nella schermata Informazioni sulla rete per risolvere i problemi di connessione su un telefono.

Se un utente ha problemi di connessione a una rete telefonica, viene visualizzato un messaggio sul telefono.

Procedura

Passaggio 1 Per visualizzare il menu Stato, premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Stato** > **Messaggi di stato**.

Passaggio 3 Selezionare **Informazioni sulla rete**.

Passaggio 4 Per uscire dalla schermata Informazioni sulla rete, premere **Esci**.

Visualizzazione della finestra Statistiche di rete

La schermata Statistiche di rete visualizza le informazioni sulle prestazioni di rete e del telefono.

Per visualizzare la schermata Statistiche di rete, attenersi alla procedura seguente:

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Stato** > **Statistiche di rete**.

Passaggio 3 Per azzerare le statistiche per Rx Frames, Tx Frames e Rx Broadcasts, premere **Cancella**.

Passaggio 4 Per uscire dalla schermata Statistiche Ethernet, premere **Esci**.

Informazioni sulle statistiche Ethernet

Nella tabella seguente vengono descritte le informazioni della schermata Statistiche Ethernet.

Tabella 42: Informazioni sulle statistiche Ethernet

Elemento	Descrizione
Rx Frames	Numero di pacchetti ricevuti dal telefono.
Tx Frames	Numero di pacchetti inviati dal telefono.
Rx Broadcasts	Numero di pacchetti broadcast ricevuti dal telefono.

Elemento	Descrizione
Motivo riavvio	Causa dell'ultima reimpostazione del telefono. Specifica uno dei valori seguenti: • Inizializzato • TCP-timeout • TCP-chiuso-DaCM • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Tel-Tastiera • Tel-Nuovo ind. IP • Reimp-Reimp • Reimp-Riavvia • Tel-Reg-Rif • Caric. HC non riuscito • CM-ICMP-Irragg • Telefono - Annulla
Tempo trascorso	Intervallo di tempo trascorso dall'ultimo riavvio del telefono.
Porta 1	Stato del collegamento e connessione della porta di rete. Ad esempio, **`Auto 100 Mb Full-Duplex`** indica che la porta di rete è in stato link-up e che ha negoziato in automatico una connessione full-duplex, 100-Mbps.
Porta 2	Stato del collegamento e connessione della porta PC.
Stato DHCP (IPv4/IPv6)	• Nella modalità solo IPv4, visualizza soltanto lo stato DHCPv4, come ad esempio DHCP BOUND. • Nella modalità IPv6, visualizza soltanto lo stato DHCPv6, come ad esempio ROUTER ADVERTISE. • Vengono visualizzate le informazioni sullo stato di DHCPv6.

Nelle tabelle seguenti vengono descritti i messaggi visualizzati per gli stati DHCPv4 e DHCPv6.

Tabella 43: Messaggi sulle statistiche Ethernet DHCPv4

Stato DHCPv4	Descrizione
CDP INIT	CDP non associato o WLAN non attiva
DHCP BOUND	DHCPv4 è in stato BOUND
DHCP DISABLED	DHCPv4 è disabilitato

Stato DHCPv4	Descrizione
DHCP INIT	DHCPv4 è in stato INIT
DHCP INVALID	DHCPv4 è in stato INVALID; (stato iniziale)
DHCP RENEWING	DHCPv4 è in stato RENEWING
DHCP REBINDING	DHCPv4 è in stato REBINDING
DHCP REBOOT	Riavvio iniziale di DHCPv4 in corso
DHCP REQUESTING	Richiesta di DHCPv4 in corso
DHCP RESYNC	DHCPv4 è in stato RESYNC
DHCP WAITING COLDBOOT TIMEOUT	Avvio di DHCPv4 in corso
DHCP UNRECOGNIZED	Stato di DHCPv4 non riconosciuto
DISABLED DUPLICATE IP	Indirizzo IPv4 duplicato
DHCP TIMEOUT	Timeout di DHCPv4
IPV4 STACK TURNED OFF	Il telefono è in modalità Solo IPv6 con lo stack IPv4 disattivato
ILLEGAL IPV4 STATE	Stato IPv4 non valido (non dovrebbe verificarsi)

Tabella 44: Messaggi sulle statistiche Ethernet DHCPv6

Stato DHCPv6	Descrizione
CDP INIT	Inizializzazione di CDP in corso
DHCP6 BOUND	DHCPv6 è in stato BOUND
DHCP6 DISABLED	DHCPv6 è in stato DISABLED
DHCP6 RENEW	Rinnovo di DHCPv6 in corso
DHCP6 REBIND	DHCPv6 è in stato REBINDING
DHCP6 INIT	Inizializzazione di DHCPv6 in corso
DHCP6 SOLICIT	Richiesta di DHCPv6 in corso
DHCP6 REQUEST	Richiesta di DHCPv6 in corso
DHCP6 RELEASING	Rilascio di DHCPv6 in corso
DHCP6 RELEASED	DHCPv6 è stato rilasciato
DHCP6 DISABLING	Disabilitazione di DHCPv6 in corso
DHCP6 DECLINING	Rifiuto di DHCPv6 in corso

Stato DHCPv6	Descrizione
DHCP6 DECLINED	Il DHCPv6 è stato rifiutato
DHCP6 INFOREQ	Il DHCPv6 è in stato INFOREQ
DHCP6 INFOREQ DONE	Il DHCPv6 è in stato INFOREQ DONE
DHCP6 INVALID	Il DHCPv6 è in stato INVALID; (stato iniziale)
DISABLED DUPLICATE IPV6	Il DHCP6 è in stato DISABLED, ma DUPLICATE IPV6 DETECTED
DHCP6 DECLINED DUPLICATE IP	Il DHCP6 è in stato DECLINED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	Indirizzo IPv6 configurato automaticamente duplicato
DHCP6 WAITING COLDBOOT TIMEOUT	Avvio di DHCPv6 in corso
DHCP6 TIMEOUT USING RESTORED VAL	Timeout di DHCPv6; è in uso il valore salvato nella memoria flash
DHCP6 TIMEOUT CANNOT RESTORE	Timeout di DHCPv6; non è presente nessun backup nella memoria flash
IPV6 STACK TURNED OFF	Il telefono è in modalità Solo IPv4 con lo stack IPv6 disattivato
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	L'indirizzo IPv6 non proviene dal router o dal server DHCPv6
ILLEGAL IPV6 STATE	Stato IPv6 non valido (non dovrebbe verificarsi)

Visualizzazione della finestra Statistiche wireless

Questa procedura si applica solo al telefono wireless telefono IP Cisco 8861.

Per visualizzare la schermata Statistiche wireless, attenersi alla procedura seguente:

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Stato** > **Statistiche wireless**.

Passaggio 3 Per reimpostare le statistiche wireless su 0, premere **Cancella**.

Passaggio 4 Per uscire dalla schermata Statistiche wireless, premere **Esci**.

Statistiche WLAN

Nella tabella seguente vengono descritte le statistiche WLAN sul telefono.

Tabella 45: Statistiche WLAN sul telefono IP Cisco Unified

Elemento	Descrizione
Byte tx	Numero di byte trasmessi dal telefono.
Byte rx	Numero di byte ricevuti dal telefono.
Pacchetti tx	Numero di pacchetti trasmessi dal telefono.
Pacchetti rx	Numero di pacchetti ricevuti dal telefono.
Pacchetti tx interrotti	Numero di pacchetti interrotti durante la trasmissione.
Pacchetti rx interrotti	Numero di pacchetti interrotti durante il ricevimento.
Errori pacchetti tx	Numero di pacchetti errati trasmessi dal telefono.
Errori pacchetti rx	Numero di pacchetti errati ricevuti dal telefono.
Tx frames	Numero di MSDU trasmessi correttamente.
Frame multicast tx	Numero di MSDU multicast trasmessi correttamente.
Nuovo tentativo tx	Numero di MSDU trasmessi correttamente dopo una o più ritrasmissioni.
Molteplici nuovi tentativi tx	Numero di MSDU multicast trasmessi correttamente dopo una o più ritrasmissioni.
Errore tx	Numero di MSDU trasmessi in modo errato poiché i tentativi di trasmissione superano il limite.
rts completato	Questo numero aumenta quando viene ricevuto un CTS in risposta a un RTS.
Errore rts	Questo numero aumenta quando un CTS non viene ricevuto in risposta a un RTS.
Errore ack	Questo numero aumenta quando un ACK non viene ricevuto quando previsto.
Frame rx duplicati	Numero di frame ricevuti indicati dal campo Controllo sequenza come duplicati.
Pacchetti rx frammentati	Numero di MPDU di tipo Dati o Gestione ricevuti correttamente.
Conteggio roaming	Numero di roaming corretti.

Visualizzazione della finestra Statistiche chiamate

È possibile accedere alla schermata Statistiche chiamate del telefono per visualizzare contatori, statistiche e metriche della qualità della voce relative alla chiamata più recente.

Nota È inoltre possibile visualizzare da remoto le informazioni sulle statistiche delle chiamate mediante un browser Web per accedere alla pagina Web Statistiche di flusso. Questa pagina Web contiene ulteriori statistiche RTCP non disponibili nel telefono.

Una singola chiamata può utilizzare più flussi vocali, ma vengono acquisiti soltanto i dati relativi al flusso vocale più recente. Un flusso vocale è un flusso di pacchetti tra due endpoint. Se un endpoint viene messo in attesa, il flusso vocale si arresta anche se la chiamata è ancora connessa. Quando si riprende la chiamata, inizia un nuovo flusso di pacchetti e i dati della nuova chiamata sovrascrivono i dati della chiamata precedente.

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Stato** > **Statistiche chiamate**.

Passaggio 3 Per uscire dalla schermata Statistiche chiamate, premere **Esci**.

Campi di Statistiche chiamate

Nella tabella seguente vengono descritte le voci visualizzate nella schermata Statistiche chiamate.

Tabella 46: Campi di Statistiche chiamate per il telefono IP Cisco Unified

Elemento	Descrizione
Codec destinatario	Tipo di flusso vocale ricevuto (audio flusso RTP dal codec): • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC

Elemento	Descrizione
Codec mittente	Tipo di flusso vocale trasmesso (audio flusso RTP dal codec): • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC
Dimensione destinatario	Dimensione dei pacchetti voce, espressa in millisecondi, nel flusso vocale di ricezione (audio flusso RTP).
Dimensione mittente	Dimensione dei pacchetti voce, espressa in millisecondi, nel flusso vocale di trasferimento.
Pacchetti destinatario	Numero di pacchetti voce RTP ricevuti dall'apertura del flusso vocale. **Nota** Questo numero non è necessariamente uguale al numero di pacchetti voce RTP ricevuti dall'inizio della chiamata, poiché la chiamata potrebbe essere stata messa in attesa.
Pacchetti mittente	Numero di pacchetti voce RTP trasmessi dall'apertura del flusso vocale. **Nota** Questo numero non è necessariamente uguale al numero di pacchetti voce RTP trasmessi dall'inizio della chiamata, poiché la chiamata potrebbe essere stata messa in attesa.
Jitter medio	Jitter medio stimato del pacchetto RTP (ritardo dinamico che può verificarsi per un pacchetto mentre si sposta nella rete), espresso in millisecondi, rilevato dall'apertura del flusso vocale di ricezione.
Jitter massimo	Jitter massimo, espresso in millisecondi, rilevato dall'apertura del flusso vocale di ricezione.
Destinatario perso	Numero di pacchetti RTP nel flusso vocale in ricezione persi (pacchetti errati, arrivati in ritardo e così via). **Nota** Il telefono ignora i pacchetti di rumore di comfort del payload di tipo 19 generati dai gateway di Cisco, poiché aumentano tale numero.
Pacchetti persi destinatario	Pacchetti RTP mancanti (persi durante il trasferimento).
Metriche di qualità audio	

Elemento	Descrizione
Indice occultamento cumulativo	Numero totale di frame di occultamento diviso per il numero totale di frame voce ricevuti dall'inizio del flusso vocale.
Indice occultamento intervallo	Rapporto tra i frame di occultamento e i frame voce nel precedente intervallo di 3 secondi della comunicazione vocale attiva. Se è in uso il rilevamento dell'attività vocale (VAD, Voice Activity Detection), può essere necessario un intervallo più lungo per accumulare 3 secondi di comunicazione vocale attiva.
Indice massimo di occultamento	Indice occultamento intervallo più alto dall'inizio del flusso vocale.
Secondi occultamento	Numero di secondi con eventi di occultamento (frame persi) dall'inizio del flusso vocale (comprende secondi di occultamento rigoroso).
Secondi occultamento rigoroso	Numero di secondi con eventi di occultamento (frame persi) superiori al 5% dall'inizio del flusso vocale.
Latenza	Stima della latenza di rete, espressa in millisecondi. Rappresenta una media progressiva del ritardo round-trip, misurata alla ricezione dei blocchi del report destinatario RTCP.

Visualizzazione della finestra Punto di accesso attuale

La schermata Punto di accesso attuale visualizza le statistiche sul punto di acceso utilizzato dal telefono IP Cisco 8861 per le comunicazioni wireless.

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Stato** > **Punto di accesso attuale**.

Passaggio 3 Per uscire dalla schermata Punto di accesso attuale, premere **Esci**.

Campi di Punto di accesso attuale

Nella tabella seguente vengono descritti i campi della schermata Punto di accesso attuale.

Tabella 47: Campi di Punto di accesso attuale

Elemento	Descrizione
Nome AP	Nome dell'AP, se conforme a CCX; in caso contrario, viene visualizzato l'indirizzo MAC.
Indirizzo MAC	L'indirizzo MAC dell'AP.
Frequenza	L'ultima frequenza in cui è stato rilevato l'AP.

Elemento	Descrizione
Canale corrente	L'ultimo canale in cui è stato rilevato l'AP.
Ultimo RSSI	L'ultimo RSSI in cui è stato rilevato l'AP.
Intervallo beacon	Numero di unità di tempo tra più beacon. Un'unità di tempo è pari a 1,024 ms.
Capacità	Questo campo contiene dei campi secondari utilizzati per indicare le capacità facoltative richieste o annunciate.
Velocità di base	Velocità dei dati richieste dall'AP e l'AP su cui la stazione deve essere in grado di operare.
Velocità opzionali	Velocità dei dati supportate dall'AP e l'AP su cui la stazione opera facoltativamente.
Velocità VHT(rx) supportate	Set RX MCS supportato da VHT ricevuto dall'AP.
Velocità VHT(tx) supportate	Set TX MCS supportato da VHT ricevuto dall'AP.
HT MCS supportati	Set MCS supportato da HT ricevuto dall'AP.
Periodo DTIM	Ogni beacon corrisponde a un periodo DTIM. Dopo ciascun beacon DTIM, l'AP invia dei pacchetti broadcast o multicast che vengono messi in coda per i dispositivi a risparmio energetico.
Codice paese	Codice paese a due cifre. Se l'elemento di informazioni (IE) del paese non è presente nel beacon, le informazioni sul paese potrebbero non essere visualizzate.
Canali	Un elenco dei canali supportati (dall'IE del paese).
Limite alimentazione	La quantità di alimentazione in base a cui è consigliabile ridurre la potenza di trasmissione massima dal limite del dominio normativo.
Limite alimentazione	Potenza di trasmissione massima in dBm consentita per un canale specifico.
Utilizzo canale	La percentuale di tempo, normalizzato su 255, in cui l'AP ha rilevato che il supporto era occupato, come indicato dal meccanismo di rilevamento della portante (CS) fisico o virtuale.
Conteggio stazioni	Il numero totale di STA attualmente associati all'AP.
Capacità di ammissione	Un numero intero senza segno che specifica il rimanente intervallo di tempo sul supporto disponibile tramite un controllo esplicito di ammissione, in unità di 32 microsecondi al secondo. Se il valore è pari a 0, l'AP non supporta questo elemento di informazione e la capacità è sconosciuta.
WMM supportato	Supporto per le estensioni multimediali Wi-Fi.

Elemento	Descrizione
UAPSD supportato	L'AP supporta l'implementazione Unscheduled Automatic Power Save Delivery. Disponibile solo se WMM è supportato. Questa funzione è di importanza critica per il tempo di chiamata e per il raggiungimento della densità di chiamata massima sul telefono IP wireless.
ARP proxy	L'AP conforme a CCX supporta la risposta alle richieste ARP IP per conto della stazione associata. Questa funzione è di importanza critica per il tempo di standby sul telefono IP wireless.
Versione CCX	Se l'AP è conforme a CCX, in questo campo viene visualizzata la versione di CCX.
Best Effort	Contiene le informazioni relative alla coda Best Effort.
Background	Contiene le informazioni relative alla coda in background.
Video	Contiene le informazioni relative alla coda video.
Voce	Contiene le informazioni relative alla coda vocale.

Pagina Web del telefono IP Cisco

Per ciascun telefono IP Cisco è disponibile di una pagina Web da cui è possibile visualizzare diverse informazioni sul telefono, tra cui:

- Informazioni dispositivo: visualizza le impostazioni del dispositivo e le relative informazioni.
- Impostazione di rete: visualizza le informazioni sull'impostazione di rete e su altre impostazioni del telefono.
- Statistiche di rete: visualizza gli hyperlink che forniscono informazioni sul traffico di rete.
- Log dei dispositivi: visualizza gli hyperlink che forniscono informazioni per la risoluzione dei problemi.
- Statistiche di flusso: visualizza gli hyperlink a diverse statistiche di flusso.
- Sistema: visualizza un hyperlink per il riavvio del telefono.

In questa sezione vengono descritte le informazioni che è possibile visualizzare sulla pagina Web del telefono. È possibile utilizzare queste informazioni per monitorare da remoto il funzionamento di un telefono e per fornire assistenza durante la risoluzione dei problemi.

È inoltre possibile visualizzare la maggior parte di queste informazioni direttamente sul telefono.

Accesso alla pagina Web del telefono

Per accedere alla pagina Web di un telefono, attenersi a questa procedura:

Nota Se non è possibile accedervi, la pagina Web potrebbe essere disabilitata per impostazione predefinita.

Procedura

Passaggio 1 Ottenere l'indirizzo IP del telefono IP Cisco tramite uno dei metodi seguenti:

a) Cercare il telefono in Cisco Unified Communications Manager Administration scegliendo **Dispositivo** > **Telefono**. Sui telefoni registrati in Cisco Unified Communications Manager viene visualizzato l'indirizzo IP nella finestra **Cerca ed elenca telefoni** e in cima alla finestra **Configurazione telefono**.

b) Sul telefono IP Cisco, premere **Applicazioni**, selezionare **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione Ethernet** > **Impostazione IPv4** e scorrere fino al campo Indirizzo IP.

Passaggio 2 Aprire un browser Web e immettere il seguente URL, dove *indirizzo_IP* è l'indirizzo IP del telefono IP Cisco:

`http://`*indirizzo_IP*

Informazioni dispositivo

Nell'area Informazioni dispositivo della pagina Web del telefono vengono visualizzate le impostazioni del dispositivo e le informazioni correlate sul telefono. La tabella che segue descrive tali voci.

Nota Alcune delle voci nella tabella seguente non sono valide per tutti i modelli di telefono.

Per visualizzare l'area **Informazioni dispositivo**, accedere alla pagina Web del telefono come descritto in Accesso alla pagina Web del telefono, a pagina 237, quindi fare clic sul collegamento ipertestuale **Informazioni dispositivo**.

Tabella 48: Voci dell'area Informazioni dispositivo

Elemento	Descrizione
Modalità servizio	La modalità di servizio del telefono.
Nome servizio	Il dominio del servizio.
Stato servizio	Lo stato corrente del servizio.
Indirizzo MAC	Indirizzo MAC (Media Access Control) del telefono.
Nome host	Nome fisso e univoco assegnato automaticamente al telefono in base all'indirizzo MAC.
Nr. rubrica tel.	Numero di rubrica assegnato al telefono.
ID applicazione installata	Versione del firmware dell'applicazione in esecuzione sul telefono.
ID applicazione di avvio	Versione del firmware di avvio.
Versione	Identificativo del firmware in esecuzione sul telefono.

Elemento	Descrizione
Modulo di espansione tasti 1	Identificatore del primo modulo di espansione tasti, se applicabile. Applicabile ai telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR.
Modulo di espansione tasti 2	Identificatore del secondo modulo di espansione tasti, se applicabile. Applicabile ai telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR.
Modulo di espansione tasti 3	Identificatore del terzo modulo di espansione tasti, se applicabile. Applicabile ai telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR.
Revisione hardware	Valore della revisione minore dell'hardware del telefono.
Numero di serie	Numero di serie unico del telefono.
Numero modello	Numero di modello del telefono.
Messaggio in attesa	Indica se è presente un messaggio vocale in attesa sulla linea principale del telefono in uso.
UDI	Visualizza le seguenti informazioni UDI (Unique Device Identifier) di Cisco sul telefono: • Tipo di dispositivo: indica il tipo di hardware. Ad esempio, viene visualizzato Telefono per tutti i modelli del telefono. • Descrizione dispositivo: visualizza il nome del telefono associato al tipo di modello indicato. • ID prodotto: specifica il modello del telefono. • ID versione (VID): specifica il numero di versione hardware principale. • Numero di serie: visualizza il numero di serie univoco del telefono.
UDI del modulo di espansione tasti	UDI (Unique Device Identifier, ID dispositivo univoco) Cisco del modulo di espansione dei tasti. Applicabile ai telefoni IP Cisco 8851, 8851NR, 8861, 8865 e 8865NR.

Elemento	Descrizione
Nome della cuffia	Visualizza il nome della cuffia Cisco collegata nella colonna a sinistra. La colonna a destra contiene le seguenti informazioni: • Porta: visualizza la modalità di collegamento della cuffia al telefono. • USB • AUX • Versione: visualizza la versione del firmware della cuffia. • Copertura radio: visualizza la potenza configurata per la radio DECT. Applicabile solo alla Cuffia Cisco serie 560. • Larghezza di banda: visualizza se la cuffia utilizza la banda larga o la banda stretta. Applicabile solo alla Cuffia Cisco serie 560. • Bluetooth: visualizza se il Bluetooth è abilitato o disabilitato. Applicabile solo alla Cuffia Cisco serie 560. • Conferenza: visualizza se la funzione conferenza è abilitata o disabilitata. Applicabile solo alla Cuffia Cisco serie 560. • Origine firmware: visualizza il metodo di aggiornamento del firmware consentito: • Limita solo a UCM • Consenti da UCM o da Cisco Cloud Applicabile solo alla Cuffia Cisco serie 560.
Ora	Ora del gruppo Data/ora a cui appartiene il telefono. Queste informazioni provengono da Cisco Unified Communications Manager.
Fuso orario	Fuso orario del gruppo Data/ora a cui appartiene il telefono. Queste informazioni provengono da Cisco Unified Communications Manager.
Data	Data del gruppo Data/ora a cui appartiene il telefono. Queste informazioni provengono da Cisco Unified Communications Manager.
Memoria sistema libera	Memoria non utilizzata sul telefono
Memoria libera heap Java	Memoria interna heap Java libera
Memoria libera pool Java	Memoria interna pool Java libera
Modalità FIPS abilitata	Indica se la modalità FIPS (Federal Information Processing Standard) è abilitata.

Impostazione di rete

Nell'area Impostazione di rete della pagina Web del telefono è possibile visualizzare le informazioni sull'impostazione della rete e su altre impostazioni del telefono. La tabella che segue descrive tali voci.

È possibile visualizzare e impostare molte di queste voci dal menu Impostazione di rete sul telefono IP Cisco.

Nota Alcune delle voci nella tabella seguente non sono valide per tutti i modelli di telefono.

Per visualizzare l'area **Impostazione di rete**, accedere alla pagina Web del telefono come descritto in Accesso alla pagina Web del telefono, a pagina 237, quindi fare clic sull'hyperlink **Impostazione di rete**.

Tabella 49: Voci dell'area Impostazione di rete

Elemento	Descrizione
Indirizzo MAC	Indirizzo MAC (Media Access Control) del telefono.
Nome host	Nome host assegnato dal server DHCP al telefono.
Nome dominio	Nome del dominio DNS (Domain Name System) in cui risiede il telefono.
Server DHCP	Indirizzo IP del server DHCP (Dynamic Host Configuration Protocol) da cui il telefono ottie IP.
Server BOOTP	Indica se il telefono ottiene la configurazione da un server BootP (Bootstrap Protocol).
DHCP	Indica se il telefono utilizza DHCP.
Indirizzo IP	Protocollo Internet (IPv4) del telefono.
Subnet mask	Subnet mask utilizzata dal telefono.
Router predefinito	Router predefinito utilizzato dal telefono.
Server DNS 1 - 3	Server DNS (Domain Name System) primario (Server DNS 1) e server DNS opzionali di ba DNS 2 e 3) utilizzati dal telefono.
TFTP alternativo	Indica se il telefono utilizza un server TFTP alternativo.
Server TFTP 1	Server TFTP (Trivial File Transfer Protocol) primario utilizzato dal telefono.
Server TFTP 2	Server TFTP (Trivial File Transfer Protocol) di backup utilizzato dal telefono.
Indirizzo DHCP rilasciato	Indica l'impostazione dell'opzione Indirizzo DHCP rilasciato nel menu Configurazione di telefono.
ID VLAN operativa	VLAN (Virtual Local Area Network) operativa configurata su uno switch Cisco Catalyst a cu il telefono.
ID VLAN amministrazione	VLAN ausiliaria a cui appartiene il telefono.

Elemento	Descrizione
Server CUCM 1 – 5	Nomi host o indirizzi IP, in ordine prioritario, dei server Cisco Unified Communications Mar cui è possibile registrare il telefono. Una voce può anche mostrare l'indirizzo IP di un router grado di fornire funzionalità di Cisco Unified Communications Manager limitata, se tale rout disponibile. Per un server disponibile, una voce mostra l'indirizzo IP del server Cisco Unified Communic Manager e uno degli stati seguenti: • Attivo: server Cisco Unified Communications Manager da cui il telefono riceve corrente servizi di elaborazione chiamate • In attesa: server Cisco Unified Communications Manager a cui passa il telefono se il server non è più disponibile • Vuoto: nessuna connessione corrente a questo server Cisco Unified Communications M Una voce può includere anche la designazione SRST (Survivable Remote Site Telephony), che i un router SRST in grado di fornire funzionalità di Cisco Unified Communications Manager c insieme limitato di funzioni. Questo router assume il controllo dell'elaborazione delle chiamat gli altri server Cisco Unified Communications Manager sono irraggiungibili. Il server Cisco Communications Manager di SRST viene visualizzato sempre come ultimo nell'elenco dei serv se è attivo. È possibile configurare l'indirizzo del router SRST nella sezione Gruppo dispositi finestra di Cisco Unified Communications Manager Configuration.
URL info	URL del testo della guida visualizzato sul telefono.
URL rubriche	URL del server da cui il telefono ottiene le informazioni sulla rubrica.
URL messaggi	URL del server da cui il telefono ottiene i servizi di messaggio.
URL servizi	URL del server da cui il telefono ottiene i servizi del telefono IP Cisco Unified.
Inattività URL	URL visualizzato dal telefono se è inattivo per il periodo specificato nel campo Tempo inattiv e non è stato aperto nessun menu.
Tempo inattività URL	Numero di secondi di inattività del telefono senza nessun menu aperto prima che il servizio X specificato da Inattività URL venga attivato.
URL server proxy	URL del server proxy, che invia le richieste HTTP agli indirizzi host non locali per conto del HTTP del telefono e fornisce risposte dall'host non locale al client HTTP del telefono.
URL di autenticazione	URL utilizzato dal telefono per convalidare le richieste fatte al server Web del telefono.
Impostazione porta SW	Velocità e duplex della porta dello switch, dove: • A = Negoziazione automatica • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • Nessun collegamento = Nessuna connessione alla porta dello switch

Elemento	Descrizione
Impostazione porta PC	Velocità e duplex della porta del PC, dove: • A = Negoziazione automatica • 10H = 10-BaseT/half duplex • 10F = 10-BaseT/full duplex • 100H = 100-BaseT/half duplex • 100F = 100-BaseT/full duplex • 1000F = 1000-BaseT/full duplex • Nessun collegamento = Nessuna connessione alla porta PC
Porta PC disattivata	Indica se la porta PC del telefono è abilitata o disabilitata.
Utente - Impostazioni internazionali	Impostazioni internazionali dell'utente associate all'utente del telefono. Identifica una seri informazioni dettagliate per il supporto degli utenti, compresi lingua, carattere, formattaz e ora e informazioni sulla tastiera alfanumerica.
Rete - Impostazioni internazionali	Impostazioni internazionali della rete associate all'utente del telefono. Identifica una serie di i dettagliate per il supporto del telefono in una ubicazione specifica, comprese definizioni cadenze utilizzati dal telefono.
Utente - Versione impostazioni internazionali	Versione delle impostazioni internazionali dell'utente caricate nel telefono.
Rete - Versione impostazioni internazionali	Versione delle impostazioni internazionali di rete caricate nel telefono.
Altoparlante abilitato	Indica se l'altoparlante è abilitato nel telefono.
GARP abilitato	Indica se il telefono apprende gli indirizzi MAC dalle risposte ARP gratuite.
Estendi a porta PC	Indica se il telefono inoltra alla porta di accesso i pacchetti trasmessi e ricevuti sulla porta
Funzionalità video abilitata	Indica se il telefono può partecipare a videochiamate quando si collega a una webcam ad equipaggiata.
VLAN voce abilitata	Indica se il telefono consente a un dispositivo collegato alla porta PC di accedere alla VL
VLAN PC abilitata	VLAN che identifica e rimuovere i tag 802.1P/Q dai pacchetti inviati al PC.
Selezione automatica linea abilitata	Identifica se il telefono seleziona automaticamente una linea quando viene sganciato il te
Controllo protocollo DSCP	Classificazione IP DSCP per la segnalazione del controllo delle chiamate.
DSCP per la configurazione	Classificazione IP DSCP per qualsiasi trasferimento di configurazione del telefono.
DSCP per i servizi	Classificazione IP DSCP per i servizi basati sul telefono.

Elemento	Descrizione
Modalità di protezione (non protetta)	Modalità di protezione impostata per il telefono.
Accesso Web abilitato	Indica se l'accesso Web è abilitato (Sì) o disabilitato (No) per il telefono.
Accesso SSH abilitato	Indica se la porta SSH è stata abilitata o disabilitata.
CDP: porta SW	Indica se il supporto CDP esiste sulla porta dello switch (abilitato per impostazione predefini Abilitare CDP sulla porta dello switch per l'assegnazione di VLAN al telefono, la negoziazio dell'alimentazione, la gestione QoS e la protezione 802.1x. Abilitare CDP sulla porta dello switch quando il telefono si collega a uno switch Cisco. Quando CDP è disabilitato in Cisco Unified Communications Manager, viene visualizzato u che indica che il CDP deve essere disabilitato sulla porta dello switch solo se il telefono si co uno switch non Cisco. I valori CDP correnti della porta dello switch e della porta PC sono visualizzati nel menu Impo
CDP: porta PC	Indica se CDP è supportato sulla porta PC (abilitato per impostazione predefinita). Quando CDP è disabilitato in Cisco Unified Communications Manager, viene visualizzato u per indicare che la disabilitazione di CDP sulla porta PC impedisce il funzionamento di CVT I valori correnti CDP della porta dello switch e della porta PC sono visualizzati nel menu Impo
LLDP-MED: porta SW	Indica se il protocollo LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discove abilitato sulla porta dello switch.
LLDP-MED: porta PC	Indica se LLDP-MED è abilitato sulla porta PC.
Priorità alimentazione LLDP	Indica la priorità di alimentazione del telefono allo switch, abilitando così lo switch per fornire energia ai telefoni. Le impostazioni comprendono: • Sconosciuto: valore predefinito. • Basso • Alto • Critico
ID dell'Asset LLDP	Identifica l'ID dell'asset assegnato al telefono per la gestione delle scorte.
File CTL	L'hash MD5 del file CTL.
File ITL	Il file ITL contiene la trust list iniziale.
Firma ITL	L'hash MD5 del file ITL.
Server CAPF	Server CPF in uso
TVS	Il componente principale di Security by Default. Trust Verification Services (TVS) consente a IP Cisco Unified di autenticare i server applicazione, come i servizi EM, rubrica e MIDlet, q stabilisce HTTPS.
Server TFTP	Il nome del server TFTP utilizzato dal telefono.

Elemento	Descrizione
Server TFTP	Il nome del server TFTP utilizzato dal telefono.
Sincronizzazione porta automatica	Indica se il telefono sincronizza automaticamente la velocità della porta per eliminare la p pacchetti.
Configurazione remota porta switch	Indica se la porta SW è controllata da remoto.
Configurazione remota porta PC	Indica se la porta PC è controllata da remoto.
Modalità indirizzi IP	Identifica la modalità di indirizzamento: • Solo IPv4 • IPv4 e IPv6 • Solo IPv6
Control. modal. Prefer. IP	Indica la versione di indirizzo IP utilizzata dal telefono durante la segnalazione con Cisco Communications Manager quando IPv4 e IPv6 sono entrambi disponibili sul telefono.
Modal. prefer. IP per supporto	
Configurazione automatica IPv6	Indica che per i supporti il dispositivo utilizza un indirizzo IPv4 per collegarsi a Cisco Un Communications Manager.
Protezione indirizzo duplicato IPv6	
Accetta messaggi reindirizzamento IPv6	Indica se il telefono accetta i messaggi di reindirizzamento dallo stesso router utilizzato p di destinazione.
Risposta richiesta echo multicast IPv6	Indica che il telefono invia un messaggio di risposta echo in risposta a un messaggio di ri inviato a un indirizzo solo IPv6.
Server di caricamento IPv6	Utilizzato per ottimizzare il tempo di installazione per gli aggiornamenti del firmware del scaricare la WAN memorizzando le immagini in locale, negando la necessità di attraversa collegamento WAN per l'aggiornamento di ogni telefono.
Server di registro IPv6	
Server CAPF IPv6	Indica porta e indirizzo IP della macchina di registrazione remota a cui il telefono invia i registro.

Elemento	Descrizione
DHCPv6	Indica il metodo utilizzato dal telefono per ottenere l'indirizzo solo IPv6. Se DHCPv6 è abilitato, il telefono ottiene l'indirizzo IPv6 o dal server DHCPv6 o dalla config automatica SLAAC dell'RA inviata dal router abilitato per IPv6. Se DHCPv6 è disabilitato, il non disporrà di nessun indirizzo IPv6 con stato (dal server DHCPv6) o senza stato (dalla config automatica SLAAC). **Nota** A differenza di DHCPv4, anche se DHCPv6 è disabilitato, il telefono può comu generare un indirizzo di configurazione automatica SLAAC se la configurazione aut è abilitata.
Indirizzo IPv6	Visualizza l'indirizzo solo IPv6 corrente del telefono. Sono supportati due formati di indirizzi: • Otto set di cifre esadecimali separati da due punti X:X:X:X:X:X:X:X • Formato compresso per comprimere un'esecuzione singola di gruppi di zero consecutivi singolo gruppo rappresentato da un doppio segno di due punti
Lunghezza prefisso IPv6	Visualizza la lunghezza del prefisso solo IPv6 corrente della subnet.
Router predefinito IPv6	Visualizza il router IPv6 predefinito utilizzato dal telefono.
Server DNS IPv6 1 - 2	Visualizza il server DNSv6 primario e secondario utilizzato dal telefono.
TFTP alternativo IPv6	Viene visualizzato se si utilizza un server TFTP IPv6 alternativo.
Server TFTP IPv6 1 - 2	Visualizza il server TFTP IPv6 primario e secondario utilizzato dal telefono.
Indirizzo IPv6 rilasciato	Indica se l'utente ha rilasciato le informazioni correlate a IPv6.
Livello energia EnergyWise	Il livello di energia utilizzata quando il telefono è inattivo.
Dominio EnergyWise	Dominio EnergyWise in cui si trova il telefono.
DF_BIT	Indica l'impostazione del bit DF per i pacchetti.

Statistiche di rete

I seguenti hyperlink alle Statistiche di rete sulla pagina Web del telefono forniscono informazioni sul traffico di rete del telefono:

- Informazioni Ethernet: visualizza le informazioni sul traffico Ethernet.
- Accesso: visualizza informazioni sul traffico di rete verso e dalla porta PC del telefono.
- Rete: visualizza informazioni sul traffico di rete verso e dalla porta di rete del telefono.

Per visualizzare l'area delle statistiche di rete, accedere alla pagina Web del telefono, quindi fare clic sull'hyperlink **Informazioni Ethernet**, **Accesso**, o **Rete**.

Pagina Web Informazioni Ethernet

Nella tabella seguente viene descritto il contenuto della pagina Web Informazioni Ethernet.

Tabella 50: Voci Informazioni Ethernet

Elemento	Descrizione
Tx Frames	Numero totale di pacchetti trasmessi dal telefono.
Tx broadcast	Numero totale di pacchetti broadcast trasmessi dal telefono.
Tx multicast	Numero totale di pacchetti multicast trasmessi dal telefono.
Tx unicast	Numero totale di pacchetti unicast trasmessi dal telefono.
Rx Frames	Numero totale di pacchetti ricevuti dal telefono
Rx broadcast	Numero totale di pacchetti broadcast ricevuti dal telefono.
Rx multicast	Numero totale di pacchetti multicast ricevuti dal telefono.
Rx unicast	Numero totale di pacchetti unicast ricevuti dal telefono.
Rx PacketNoDes	Numero totale di pacchetti shed provocati dal descrittore DMA (Direct Memory Access).

Pagine Web Accesso e Rete

Nella tabella seguente vengono descritte le informazioni contenute nelle pagine Web Accesso e Rete.

Tabella 51: Campi di Accesso e Rete

Elemento	Descrizione
Rx totalPkt	Numero totale di pacchetti ricevuti dal telefono.
Rx crcErr	Numero totale di pacchetti ricevuti con errore CRC.
Rx alignErr	Numero totale di pacchetti tra 64 e 1522 byte di lunghezza ricevuti e con FCS (Frame Check Sequence) errato.
Rx multicast	Numero totale di pacchetti multicast ricevuti dal telefono.
Rx broadcast	Numero totale di pacchetti broadcast ricevuti dal telefono.
Rx unicast	Numero totale di pacchetti unicast ricevuti dal telefono.
Rx shortErr	Numero totale di pacchetti con errore FCS ricevuti o di pacchetti con errore di allineamento con dimensione inferiore a 64 byte.
Rx shortGood	Numero totale di pacchetti corretti ricevuti con dimensione inferiore a 64 byte.
Rx longGood	Numero totale di pacchetti corretti ricevuti con dimensione superiore a 1522 byte.

Elemento	Descrizione
Rx longErr	Numero totale di pacchetti con errore FCS ricevuti o di pacchetti con errore di allineamento con dimensione superiore a 1522 byte.
Rx size64	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 0 e 64 byte.
Rx size65to127	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 65 e 127 byte.
Rx size128to255	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 128 e 255 byte.
Rx size256to511	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 256 e 511 byte.
Rx size512to1023	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 512 e 1023 byte.
Rx size1024to1518	Numero totale di pacchetti ricevuti, compresi i pacchetti errati, di dimensione compresa tra 1024 e 1518 byte.
Rx tokenDrop	Numero totale di pacchetti abbandonati a causa di risorse insufficienti (ad esempio, overflow FIFO).
Tx excessDefer	Numero totale di pacchetti trasmessi in ritardo a causa del supporto occupato.
Tx lateCollision	Numero di volte in cui si sono verificate collisioni successive a 512 bit volte dopo l'avvio della trasmissione del pacchetto.
Tx totalGoodPkt	Numero totale di pacchetti corretti (multicast, broadcast e unicast) ricevuti dal telefono.
Tx Collisions	Numero totale di collisioni verificate durante la trasmissione di un pacchetto.
Tx excessLength	Numero totale di pacchetti non trasmessi in quanto il pacchetto ha riscontrato 16 tentativi di trasmissione.
Tx broadcast	Numero totale di pacchetti broadcast trasmessi dal telefono.
Tx multicast	Numero totale di pacchetti multicast trasmessi dal telefono.
LLDP FramesOutTotal	Numero totale di frame LLDP inviati dal telefono.
LLDP AgeoutsTotal	Numero totale di frame LLDP con timeout nella cache.
LLDP FramesDiscardedTotal	Numero totale di frame LLDP ignorati quando uno dei TLV obbligatori è risultato mancante, non funzionante o contenente una lunghezza della stringa fuori intervallo.
LLDP FramesInErrorsTotal	Numero totale di frame LLDP ricevuti con uno o più errori rilevabili.

Elemento	Descrizione
LLDP FramesInTotal	Numero totale di frame LLDP ricevuti dal telefono.
LLDP TLVDiscardedTotal	Numero totale di TLV LLDP ignorati.
LLDP TLVUnrecognizedTotal	Numero totale di TLV LLDP non riconosciuti sul telefono.
ID dispositivo adiacente CDP	Identificativo di un dispositivo collegato a questa porta rilevato da CDP.
Indirizzo IPv6 adiacente CDP	Indirizzo IP del dispositivo adiacente rilevato dal protocollo CDP.
Porta adiacente CDP	Porta del dispositivo adiacente a cui è collegato il telefono rilevato dal protocollo CDP.
ID dispositivo adiacente LLDP	Identificativo di un dispositivo collegato a questa porta rilevato dal protocollo LLDP.
Indirizzo IPv6 adiacente LLDP	Indirizzo IP del dispositivo adiacente rilevato dal protocollo LLDP.
Porta adiacente LLDP	Porta del dispositivo adiacente a cui è collegato il telefono rilevato dal protocollo LLDP.
Informazioni porta	Informazioni su velocità e duplex.

Log dei dispositivi

I seguenti hyperlink al registro del dispositivo sulla pagina Web del telefono forniscono informazioni che consentono di monitorare e risolvere eventuali problemi del telefono.

- Registri console: comprende hyperlink ai singoli file di registro. I file di registro console comprendono messaggi di debug ed errore ricevuti dal telefono.
- Dump della memoria: comprende hyperlink ai singoli file di dettagli. I file dump della memoria comprendono i dati di un guasto del telefono.
- Messaggi di stato: visualizza i 10 messaggi di stato più recenti generati dal telefono dall'ultima accensione. Anche la schermata dei messaggi di stato sul telefono visualizza queste informazioni.
- Visualizzazione debug: visualizza i messaggi di debug che possono essere utili a Cisco TAC (Technical Assistance Center) se è necessaria assistenza per la risoluzione dei problemi.

Statistiche di flusso

Il telefono IP Cisco Unified è in grado di trasmettere informazioni verso e da un massimo di tre dispositivi contemporaneamente. Durante una chiamata o l'esecuzione di un servizio che invia o riceve audio o dati, in telefono trasmette informazioni.

Le aree Statistiche di flusso sulla pagina Web del telefono forniscono informazioni sui flussi.

Nella tabella seguente vengono descritte le voci delle aree Statistiche di flusso.

Tabella 52: Voci dell'area Statistiche di flusso

Elemento	Descrizione
Indirizzo remoto	Indirizzo IP e porta UDP della destinazione del flusso.
Indirizzo locale	Indirizzo IP e porta UDP del telefono.
Ora inizio	L'indicatore di data/ora interno indica quando Cisco Unified Communications Manager richiesto l'inizio della trasmissione dei pacchetti da parte del telefono.
Stato flusso	Indicazione dell'eventuale attivazione del flusso.
Nome host	Nome fisso e univoco assegnato automaticamente al telefono in base all'indirizzo MAC
Pacchetti mittente	Numero totale di pacchetti dati RTP trasmessi dal telefono dall'avvio della connessione. Il è 0 se la connessione è impostata sulla modalità di sola ricezione.
Ottetti mittente	Numero totale di ottetti di payload trasmessi dal telefono nei pacchetti dati RTP dall'avvi connessione. Il valore è 0 se la connessione è impostata sulla modalità di sola ricezione
Codec mittente	Tipo di codifica audio per il flusso di trasmissione.
Report mittente inviati (vedere nota)	Numero di volte per cui è stato inviato il report mittente RTCP.
Ora di invio report mittente (vedere nota)	Indicazione dell'indicatore di data/ora interno relativo all'ultimo invio del rapporto mitt RTCP.
Pacchetti persi destinatario	Numero totale di pacchetti dati RTP persi dall'avvio del ricevimento dati su questa conne Definito come il numero di pacchetti attesi meno il numero di pacchetti effettivamente ri dove il numero di pacchetti ricevuti comprende eventuali pacchetti in ritardo o duplicat valore è 0 se la connessione è impostata sulla modalità di solo invio.
Jitter medio	Stima della deviazione media del tempo di interarrivo del pacchetto dati RTP, misurato millisecondi. Il valore è 0 se la connessione è impostata sulla modalità di solo invio.
Codec destinatario	Tipo di codifica audio utilizzato per il flusso ricevuto.
Report destinatario inviati (vedere nota)	Numero di volte per cui sono stati inviati i report destinatario RTCP.
Ora di invio report destinatario (vedere nota)	Indicazione dell'indicatore di data/ora interno relativo all'invio del report destinatario R
Pacchetti destinatario	Numero totale di pacchetti dati RTP ricevuti dal telefono dall'avvio del ricevimento dat questa connessione. Include i pacchetti ricevuti da origini diverse, se questa chiamata è multicast. Il valore è 0 se la connessione è impostata sulla modalità di solo invio.
Ottetti destinatario	Numero totale di ottetti di payload ricevuti dal dispositivo nei pacchetti dati RTP dall'a della ricezione sulla connessione. Include i pacchetti ricevuti da origini diverse, se ques chiamata è di tipo multicast. Il valore è 0 se la connessione è impostata sulla modalità d invio.

Elemento	Descrizione
MOS LQK	Punteggio considerato come stima oggettiva del MOS (Mean Opinion Score) relativo di ascolto (LQK) valutata da 5 (eccellente) a 1 (scarsa). Questo punteggio si basa su di occultamento acustici nella perdita di frame nel precedente intervallo di otto secc flusso vocale. Per ulteriori informazioni, consultare Monitoraggio della qualità audi 280. **Nota** Il punteggio MOS LQK può variare in base al tipo di codec utilizzato da IP Cisco Unified.
Medio MOS LQK	Punteggio MOS LQK medio osservato per l'intero flusso vocale.
Min MOS LQK	Punteggio MOS LQK minimo osservato dall'inizio del flusso vocale.
Max MOS LQK	Punteggio MOS LQK massimo o baseline osservato dall'inizio del flusso vocale. In condizioni normali, questi codec forniscono il seguente punteggio MOS LQK mass perdita di frame: • G.711 porta a un punteggio di 4,5. • G.729 A/AB porta a un punteggio di 3,7.
Versione MOS LQK	Versione dell'algoritmo proprietario di Cisco utilizzato per calcolare i punteggi MO
Indice occultamento cumulativo	Numero di frame di occultamento diviso per il numero totale di frame voce ricevuti del flusso vocale.
Indice occultamento intervallo	Rapporto tra i frame di occultamento con i frame voce nel precedente intervallo di 3 della comunicazione vocale attiva. Se è in uso il rilevamento dell'attività vocale (VA Activity Detection), può essere necessario un intervallo più lungo per accumulare tr di comunicazione vocale attiva.
Indice massimo di occultamento	Indice occultamento intervallo più alto dall'inizio del flusso vocale.
Secondi occultamento	Numero di secondi con eventi di occultamento (frame persi) dall'inizio del flusso vo (comprende secondi di occultamento rigoroso).
Secondi occultam. rigoroso	Numero di secondi con eventi di occultamento di oltre il cinque percento (frame persi) del flusso vocale.
Latenza (vedere nota)	Stima della latenza di rete, espressa in millisecondi. Rappresenta una media progres ritardo round-trip, misurata alla ricezione dei blocchi del report destinatario RTCP.
Jitter massimo	Valore massimo del jitter istantaneo, espresso in millisecondi.
Dimensione mittente	Dimensione del pacchetto RTP, espressa in millisecondi, per il flusso trasmesso.
Report mittente ricevuti (vedere nota)	Numero di volte in cui i report mittente RTCP sono stati ricevuti.
Ora di ricezione report mittente (vedere nota)	Ora di ricezione più recente di un report mittente RTCP.

Elemento	Descrizione
Dimensione destinatario	Dimensione pacchetto RTP, espressa in millisecondi, per il flusso ricevuto.
Destinatario perso	Pacchetti RTP ricevuti dalla rete ma scartati dai buffer del jitter.
Report destinatario ricevuti (vedere nota)	Numero di volte in cui sono stati ricevuti i report destinatario RTCP.
Ora di ricezione report destinatario (vedere nota)	Ora di ricezione più recente di un report destinatario RTCP.
Destinatario crittografato	Indica se il destinatario utilizza la crittografia.
Mittente crittografato	Indica se il mittente utilizza la crittografia.
Fotogrammi mittente	Numero di fotogrammi inviati.
Fotogrammi parziali mittente	Numero di fotogrammi parziali inviati.
Iframe mittente	Numero di iframe inviati. Gli iframe vengono utilizzati nella trasmissione video.
IDR Frames mittente	Numero di frame IDR (Instantaneous Decoder Refresh). I frame IDR vengono utilizzat trasmissione video.
Frequenza fotogrammi mittente	Frequenza alla quale il mittente invia i fotogrammi.
Larghezza di banda mittente	Larghezza di banda per il mittente.
Risoluzione mittente	Risoluzione video del mittente.
Fotogrammi destinatario	Numero di fotogrammi ricevuti
Fotogrammi parziali destinatario	Numero di fotogrammi parziali ricevuti.
IFrame destinatario	Numero di iframe ricevuti.
IDR Frames destinatario	Numero di frame IDR ricevuti.
Richiesta IFrames destinatario	Numero di frame IDR richiesti ricevuti
Frequenza fotogrammi destinatario	Frequenza alla quale il destinatario riceve i fotogrammi.
Fotogrammi persi destinatario	Numero di fotogrammi che non sono stati ricevuti.
Errori fotogrammi destinatario	Numero di fotogrammi che non sono stati ricevuti.
Larghezza di banda destinatario	Larghezza di banda del destinatario.
Risoluzione destinatario	Risoluzione video del destinatario.
Domain	Dominio in cui risiede il telefono.

Elemento	Descrizione
Flussi trasmessi	Numero di volte che il mittente ha trasmesso flussi.
Flussi ricevuti	Numero di volte che il destinatario ha trasmesso flussi.
Flussi terminati	Numero di fotogrammi «terminati».
Ora inizio mittente	Ora di inizio del mittente.
Ora inizio destinatario	Ora di inizio del destinatario.
Stato riga	Se il telefono sta inviando un flusso.
Codifica audio mittente	Tipo di codifica audio utilizzato per il flusso.
Report mittente	Report mittente RTCP.
Ora report mittente	Ultima volta in cui è stato inviato un Report mittente RTCP.
Jitter destin	Jitter massimo del flusso.
Codifica audio destin	Tipo di codifica audio utilizzato per il flusso.
Report destinatario	Numero accessi al report delle statistiche di flusso dalla pagina Web.
Ora report destinatario	Indicatore di data / ora interno che riporta quando è stato generato il report delle sta flusso
Video Is	Indica se la chiamata è stata una videochiamata o solo audio.
ID chiamata	Identificazione della chiamata.
ID gruppo	Identificazione del gruppo in cui si trova il telefono.

Nota Se il protocollo di controllo RTP è disabilitato, non viene generato nessun dato per questo campo e viene quindi visualizzato un valore pari a 0.

Richiesta di informazioni dal telefono in formato XML

È possibile richiedere delle informazioni dal telefono per la risoluzione dei problemi. Le informazioni ricevute saranno in formato XML. Sono disponibili le seguenti informazioni:

- CallInfo indica le informazioni sulla sessione di chiamata per una linea specifica.
- LineInfo indica le informazioni di configurazione del telefono.
- ModeInfo indica le informazioni sulla modalità attivata nel telefono.

Prima di iniziare

Per ottenere le informazioni, è necessario che l'accesso Web sia abilitato.

Il telefono deve essere associato a un utente.

Procedura

Passaggio 1 Per Info chiamata, immettere nel browser l'URL seguente: **http://<phone ip address>/CGI/Java/CallInfo<x>**

dove

- <*phone ip address*> è l'indirizzo IP del telefono
- per <*x*> si intende il numero di linea su cui ricevere le informazioni.

Il comando restituisce un documento XML.

Passaggio 2 Per Info chiamata, immettere nel browser l'URL seguente: **http://<phone ip address>/CGI/Java/LineInfo**

dove

- <*phone ip address*> è l'indirizzo IP del telefono

Il comando restituisce un documento XML.

Passaggio 3 Per Info modello, immettere nel browser l'URL seguente: **http://<phone ip address>/CGI/Java/ModelInfo**

dove

- <*phone ip address*> è l'indirizzo IP del telefono

Il comando restituisce un documento XML.

Output CallInfo di esempio

Il codice XML seguente è un esempio dell'output del comando CallInfo.

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
```

```
      <CallReference>30303060</CallReference>
      <CallDuration>12835</CallDuration>
      <CallStatus>null</CallStatus>
      <CallSecurity>UNAUTHENTICATED</CallSecurity>
      <CallPrecedence>ROUTINE</CallPrecedence>
      <FeatureList/>
    </CiscoIPPhoneCallInfo>
    <VisibleFeatureList>
      <Feature Position="1" Enabled="true" Label="End Call"/>
      <Feature Position="2" Enabled="true" Label="Show Detail"/>
    </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

Output LineInfo di esempio

Il codice XML seguente è un esempio dell'output del comando LineInfo.

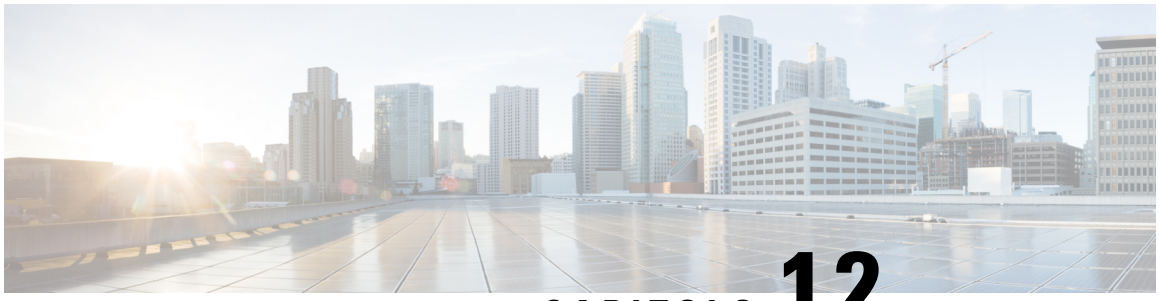
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1030</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>CONNECTED</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>2</LineType>
     <lineDirNum>9700</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <LineLabel>SD9700</LineLabel>
     <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

Output ModeInfo di esempio

Il codice XML seguente è un esempio dell'output del comando ModeInfo.

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
```

```
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



CAPITOLO 12

Risoluzione dei problemi

Informazioni generali sulla risoluzione dei problemi

Nella tabella che segue vengono fornite informazioni generali sulla risoluzione dei problemi per il telefono IP Cisco.

Tabella 53: Risoluzione dei problemi del telefono IP Cisco

Riepilogo	Spiegazione
Collegamento di un telefono IP Cisco a un altro telefono IP Cisco	Cisco non supporta il collegamento di un telefono IP a un altro attraver PC. Ciascun telefono IP deve essere collegato direttamente a una porta I telefoni, se sono collegati insieme in una linea tramite la porta PC, nor
Disturbi di trasmissione prolungati causano il ripristino dei telefoni IP oppure impediscono di effettuare o rispondere alle chiamate	Disturbi di trasmissione di Livello 2 prolungati (che durano diversi mi VLAN vocale causano il ripristino dei telefoni IP, la perdita di una chia o l'impossibilità di avviare o rispondere a una chiamata. I telefoni posson attivi fino al termine dei disturbi di trasmissione.

Riepilogo	Spiegazione
Spostamento di una connessione di rete dal telefono a una postazione di lavoro	Se si alimenta il telefono tramite connessione di rete, occorre procedere con a se si decide di scollegare la connessione di rete del telefono e collegare il c computer desktop. **Attenzione** La scheda di rete nel computer non può ricevere l'alimentazio attraverso la connessione di rete; se l'alimentazione proviene c connessione, la scheda di rete può venire distrutta. Per protegg scheda di rete, attendere almeno 10 secondi dopo aver scollegat dal telefono prima di collegarlo al computer. Questo intervallo sufficiente affinché lo switch rilevi l'assenza del telefono sulla interrompa la fornitura di energia al cavo.
Modifica della configurazione del telefono	Per impostazione predefinita, le opzioni di configurazione della rete sono b per impedire agli utenti di apportare modifiche che possono influire sulla co di rete. Prima di poterle configurare, occorre sbloccare le opzioni di config della rete. Per informazioni, vedere Applicazione di una password al telefo pagina 50. **Nota** Se la password dell'amministratore non è impostata nel profilo telefono comune, l'utente può modificare le impostazioni di re
Mancata corrispondenza del codec tra il telefono e un altro dispositivo	Le statistiche RxType e TxType mostrano il codec utilizzato per una conve tra il telefono IP Cisco in uso e un altro dispositivo. I valori di queste statis devono corrispondere. In caso contrario, verificare che l'altro dispositivo pos la conversazione codec o che sia presente un transcoder per gestire il servi
Mancata corrispondenza del campione audio tra il telefono e un altro dispositivo	Le statistiche RxType e TxType mostrano la dimensione dei pacchetti voce in una conversazione tra il telefono IP Cisco in uso e un altro dispositivo. I queste statistiche devono corrispondere.
Condizione di loopback	Può verificarsi una condizione di loopback quando vengono soddisfatte le c seguenti: • L'opzione Configurazione porta SW nel menu Configurazione di rete de è impostata su 10 Half (10-BaseT/half duplex). • Il telefono è alimentato da un alimentatore esterno. • Il telefono non è alimentato (l'alimentatore è scollegato). In questo caso, la porta dello switch del telefono può disabilitarsi e il mess seguente viene visualizzato sul registro console dello switch: HALF_DUX_COLLISION_EXCEED_THRESHOLD Per risolvere questo problema, abilitare nuovamente la porta dallo switch.

Problemi di avvio

Dopo averlo installato sulla rete e aggiunto a Cisco Unified Communications Manager, il telefono dovrebbe avviarsi come descritto nel relativo argomento riportato di seguito.

Se il telefono non si avvia correttamente, consultare le sezioni seguenti per informazioni sulla risoluzione dei problemi.

Argomenti correlati

Verifica dell'avvio del telefono, a pagina 66

Il telefono IP Cisco non segue la normale procedura di avvio

Problema

Quando si collega un telefono IP Cisco alla porta di rete, il telefono non segue la normale procedura di avvio descritta nel relativo argomento e sullo schermo del telefono non viene visualizzata nessuna informazione.

Causa

Le cause di tale comportamento potrebbero essere dovute a cavi difettosi, connessioni di bassa qualità, interruzioni di rete, mancanza di alimentazione o malfunzionamento del telefono.

Soluzione

Per stabilire se si tratta di un malfunzionamento del telefono, seguire i suggerimenti riportati di seguito per escludere altri possibili problemi.

- Verificare che la porta di rete sia funzionante:
  - Sostituire i cavi Ethernet con altri cavi sicuramente funzionanti.
  - Scollegare un telefono IP Cisco funzionante da un'altra porta e connetterlo alla porta di rete in uso per verificare che sia attiva.
  - Connettere il telefono IP Cisco con problemi di avvio a un'altra porta di rete sicuramente funzionante.
  - Connettere il telefono IP Cisco con problemi di avvio direttamente alla porta sullo switch, eliminando la connessione al patch panel dell'ufficio.
- Verificare che il telefono sia collegato a una fonte di alimentazione:
  - Se si sta utilizzando una fonte di alimentazione esterna, verificare che la presa elettrica sia funzionante.
  - Se si sta utilizzando una fonte di alimentazione per interni, passare a un alimentatore esterno.
  - Se si sta utilizzando un alimentatore esterno, cambiarlo con un'unità sicuramente funzionante.
- Se il telefono continua a non avviarsi correttamente, accenderlo dall'immagine software di backup.
- Se il telefono continua a non avviarsi correttamente, effettuare un ripristino delle impostazioni predefinite.
- Se dopo aver provato queste soluzioni sullo schermo del telefono IP Cisco non viene visualizzato nessun carattere dopo almeno cinque minuti, contattare un rappresentante del supporto tecnico di Cisco per ricevere ulteriore assistenza.

Argomenti correlati

Verifica dell'avvio del telefono, a pagina 66

Impossibile effettuare la registrazione del telefono IP Cisco su Cisco Unified Communications Manager

L'avvio del telefono non avviene correttamente se, in seguito al primo passaggio del processo di avvio (quando i pulsanti LED lampeggiano), sullo schermo del telefono continuano a essere visualizzati in sequenza i messaggi iniziali. Il telefono non è in grado di avviarsi correttamente se non viene connesso alla rete Ethernet e registrato su un server di Cisco Unified Communications Manager.

Inoltre, i problemi di protezione possono impedire l'avvio corretto del telefono. Per ulteriori informazioni, vedere Procedure di risoluzione dei problemi, a pagina 269.

Il telefono visualizza messaggi di errore

Problema

Durante l'avvio, vengono segnalati degli errori nei messaggi di stato.

Soluzione

Mentre è in corso il processo di avvio del telefono, è possibile accedere ai messaggi di stato per visualizzare delle informazioni sulla causa del problema.

Argomenti correlati

Visualizzazione della finestra Messaggi di stato, a pagina 223

Il telefono non è in grado di connettersi al server TFTP o a Cisco Unified Communications Manager

Problema

Se la rete tra il telefono e il server TFTP o Cisco Unified Communications Manager non è attiva, il telefono non è in grado di avviarsi correttamente.

Soluzione

Assicurarsi che la rete sia attualmente in esecuzione.

Il telefono non è in grado di connettersi al server TFTP

Problema

Le impostazioni del server TFTP potrebbero non essere corrette.

Soluzione

Verificare le impostazioni TFTP.

Argomenti correlati

Verifica delle impostazioni TFTP, a pagina 270

Il telefono non è in grado di connettersi al server

Problema

I campi dell'indirizzamento IP e di routing potrebbero non essere stati configurati correttamente.

Soluzione

Verificare le impostazioni di indirizzamento IP e routing sul telefono. Se si sta utilizzando DHCP, tali valori dovrebbero essere forniti dal server DHCP. Se al telefono è stato assegnato un indirizzo IP statico, è necessario inserire questi valori manualmente.

Il telefono non è in grado di connettersi tramite DNS

Problema

Le impostazioni DNS potrebbero essere errate.

Soluzione

Se si utilizza il DNS per accedere al server TFTP o a Cisco Unified Communications Manager, assicurarsi di specificare un server DNS.

Mancata esecuzione di Cisco Unified Communications Manager e dei servizi TFTP

Problema

Se Cisco Unified Communications Manager o i servizi TFTP non sono in esecuzione, i telefoni potrebbero non avviarsi correttamente. In questo caso, è molto probabile che si stia verificando un errore a livello di sistema e pertanto i telefoni e i dispositivi non riescono ad avviarsi correttamente.

Soluzione

Se il servizio Cisco Unified Communications Manager non è in esecuzione, saranno influenzati tutti i dispositivi sulla rete che si affidano a quest'ultimo per effettuare delle chiamate telefoniche. Se il servizio TFTP non è in esecuzione, più dispositivi potrebbero non avviarsi correttamente. Per ulteriori informazioni, consultare Avvio del servizio, a pagina 273.

File di configurazione danneggiato

Problema

Se continuano a verificarsi dei problemi con il telefono nonostante i suggerimenti contenuti in questo capitolo, il file di configurazione potrebbe essere danneggiato.

Soluzione

Creare un nuovo file di configurazione del telefono.

Registrazione del telefono su Cisco Unified Communications Manager

Problema

Il telefono non viene registrato su Cisco Unified Communications Manager.

Soluzione

È possibile registrare un telefono IP Cisco sul server Cisco Unified Communications Manager soltanto se il telefono viene aggiunto al server o se è abilitata la registrazione automatica. Rivedere le informazioni e le procedure in Metodi di aggiunta del telefono, a pagina 73 per assicurarsi che il telefono sia stato aggiunto al database di Cisco Unified Communications Manager.

Per verificare che il telefono si trovi all'interno del database di Cisco Unified Communications Manager, selezionare **Dispositivo** > **Telefono** da Cisco Unified Communications Manager Administration. Fare clic su **Trova** per cercare il telefono in base all'indirizzo MAC. Per informazioni su come trovare l'indirizzo MAC, consultare Individuazione dell'indirizzo MAC del telefono, a pagina 72.

Se il telefono si trova già all'interno del database di Cisco Unified Communications Manager, il file di configurazione potrebbe essere danneggiato. Per assistenza, consultare File di configurazione danneggiato, a pagina 261.

Impossibile ottenere l'indirizzo IP sul telefono IP Cisco

Problema

Se un telefono non è in grado di ottenere un indirizzo IP all'avvio, potrebbe non trovarsi sulla stessa rete o sulla stessa VLAN del server DHCP oppure la porta dello switch alla quale tale telefono si connette potrebbe essere disabilitata.

Soluzione

Assicurarsi che la rete o la VLAN a cui il telefono si connette disponga dell'accesso al server DHCP e che la porta dello switch sia abilitata.

Telefono non registrato

Problema

Sullo schermo del telefono viene visualizzato il messaggio "Immettere il codice di attivazione o il dominio servizio".

Soluzione

Il telefono non dispone di un indirizzo TFTP. Verificare che l'opzione 150 fornita dal server DHCP o un TFTP alternativo venga configurata manualmente.

Problemi di reimpostazione del telefono

Se gli utenti segnalano la reimpostazione del telefono durante le chiamate o mentre il telefono è inattivo, è necessario investigare sulle cause del problema. Se la connessione di rete e la connessione di Cisco Unified Communications Manager sono stabili, il telefono non dovrebbe reimpostarsi.

In genere, un telefono si reimposta se non è in grado di connettersi alla rete o a Cisco Unified Communications Manager.

Il telefono si reimposta a causa di interruzioni di rete a intermittenza

Problema

Potrebbero essere in corso delle interruzioni di rete a intermittenza.

Soluzione

Le interruzioni di rete a intermittenza influiscono sul traffico vocale e di dati in modo diverso. Potrebbero essere in corso delle interruzioni a intermittenza non rilevate sulla rete. In tal caso, il traffico di dati riesce a inviare di nuovo i pacchetti persi, verificando che i pacchetti siano ricevuti e trasmessi. Al contrario, il traffico vocale non è in grado di recuperare i pacchetti persi. Invece di trasmettere nuovamente una connessione di rete persa, il telefono si reimposta e tenta di rieseguire la connessione alla rete. Contattare l'amministratore del sistema per informazioni sui problemi noti nella rete dei servizi voce.

Il telefono viene reimpostato a causa di errori dell'impostazione DHCP

Problema

Le impostazioni DHCP potrebbero essere errate.

Soluzione

Verificare di aver configurato correttamente il telefono per l'uso di DHCP. Verificare che il server DHCP sia impostato correttamente. Verificare la durata del lease DHCP. Si consiglia di impostare la durata del lease su 8 giorni.

Il telefono si reimposta a causa di un indirizzo IP statico errato

Problema

L'indirizzo IP statico assegnato al telefono potrebbe non essere corretto.

Soluzione

Se al telefono è stato assegnato un indirizzo IP statico, verificare di aver immesso le impostazioni corrette.

Il telefono si reimposta durante l'uso intenso della rete

Problema

Se il telefono si reimposta durante l'uso intenso della rete, è possibile che non sia stata configurata nessuna VLAN vocale.

Soluzione

L'isolamento dei telefoni su una VLAN ausiliaria separata aumenta la qualità del traffico vocale.

Il telefono si reimposta a causa di una reimpostazione volontaria

Problema

Se più utenti dispongono dell'accesso a Cisco Unified Communications Manager come amministratori, è necessario verificare che nessun altro utente abbia intenzionalmente ripristinato i telefoni.

Soluzione

È possibile verificare se il telefono IP Cisco ha ricevuto un comando di reimpostazione da Cisco Unified Communications Manager premendo **Applicazioni** sul telefono e selezionando **Impostazioni amministratore** > **Stato** > **Statistiche di rete**.

- Se nel campo Motivo riavvio viene visualizzato `Reimp-Reimp`, il telefono riceve il comando Reimp/Reimp da Cisco Unified Communications Manager Administration.
- Se nel campo Motivo riavvio viene visualizzato `Reimp-Riavvia`, il telefono si spegne perché ha ricevuto il comando Reimp/Riavvia da Cisco Unified Communications Manager Administration.

Il telefono si reimposta a causa di problemi con il DNS o di altri problemi di connettività

Problema

Il telefono continua a reimpostarsi probabilmente a causa di problemi con il DNS o di altri problemi di connettività.

Soluzione

Se il telefono continua a reimpostarsi, eliminare gli errori del DNS o altri errori di connettività seguendo la procedura riportata in Individuazione dei problemi di connettività o con il DNS, a pagina 271.

Il telefono non si accende

Problema

Sembra che il telefono non sia acceso.

Soluzione

Nella maggior parte dei casi, i telefoni si riavviano se vengono accesi tramite una fonte di alimentazione esterna ma perdono tale connessione e passano su PoE. Allo stesso modo, i telefoni possono riavviarsi se vengono accesi tramite PoE e vengono poi collegati a una fonte di alimentazione esterna.

Il telefono non è in grado di connettersi alla LAN

Problema

La connessione fisica alla LAN potrebbe essere danneggiata.

Soluzione

Verificare che la connessione Ethernet a cui si connette il telefono IP Cisco sia funzionante. Ad esempio, controllare se la porta o lo switch a cui è collegato il telefono sono inattivi e che non sia in corso il riavvio dello switch. Assicurarsi inoltre che i cavi non siano danneggiati.

Problemi di protezione del telefono IP Cisco

Nelle sezioni seguenti vengono fornite delle informazioni sulla risoluzione dei problemi relativi alle funzioni di protezione del telefono IP Cisco. Per informazioni sulle soluzioni a questi problemi e per altre informazioni sulla risoluzione dei problemi di protezione, consultare la *Guida alla protezione di Cisco Unified Communications Manager*.

Problemi relativi al file CTL

Nelle sezioni seguenti viene descritta la risoluzione dei problemi relativi al file CTL.

Errore di autenticazione; il telefono non è in grado di autenticare il file CTL

Problema

Si verifica un errore di autenticazione del dispositivo.

Causa

Il certificato di Cisco Unified Communications Manager nel file CTL è errato o inesistente.

Soluzione

Installare un certificato corretto.

Il telefono non è in grado di autenticare il file CTL

Problema

Il telefono non è in grado di autenticare il file CTL.

Causa

Il token di sicurezza con cui è stato firmato il file CTL aggiornato non esiste nel file CTL presente sul telefono.

Soluzione

Modificare il token di sicurezza nel file CTL e installare il nuovo file sul telefono.

È possibile autenticare il file CTL, ma non gli altri file di configurazione

Problema

Il telefono non è in grado di autenticare i file di configurazione diversi dal file CTL.

Causa

È presente un record TFTP errato o il file di configurazione potrebbe non essere stato firmato dal certificato corrispondente nella Trust List del telefono.

Soluzione

Controllare il record TFTP e il certificato nella Trust List.

È possibile autenticare il file ITL, ma non gli altri file di configurazione

Problema

Il telefono non è in grado di autenticare i file di configurazione diversi dal file ITL.

Causa

Il file di configurazione potrebbe non essere stato firmato dal certificato corrispondente nella Trust List del telefono.

Soluzione

Firmare nuovamente il file di configurazione utilizzando il certificato corretto.

Errore di autorizzazione TFTP

Problema

Il telefono segnala un errore dell'autorizzazione TFTP.

Causa

L'indirizzo TFTP del telefono non esiste nel file CTL.

Se è stato creato un nuovo file CTL con un nuovo record TFTP, il file CTL esistente sul telefono potrebbe non contenere un record per il nuovo server TFTP.

Soluzione

Verificare la configurazione dell'indirizzo TFTP nel file CTL del telefono.

Impossibile effettuare la registrazione del telefono

Problema

Non è possibile effettuare la registrazione del telefono su Cisco Unified Communications Manager.

Causa

Il file CTL non contiene le informazioni corrette relative al server Cisco Unified Communications Manager.

Soluzione

Modificare le informazioni relative al server Cisco Unified Communications Manager nel file CTL.

File di configurazione firmati non richiesti

Problema

Il telefono non richiede i file di configurazione firmati.

Causa

Il file CTL non contiene nessuna voce TFTP con certificati.

Soluzione

Configurare le voci TFTP con certificati nel file CTL.

Problemi con le videochiamate

Video non disponibile tra due videotelefoni IP Cisco

Problema

Streaming assente tra due videotelefoni IP Cisco.

Soluzione

Assicurarsi che nessun punto MTP (Media Termination Point) sia in uso durante il flusso della chiamata.

Video discontinuo o saltano fotogrammi

Problema

Durante una videochiamata, il video è discontinuo o saltano i fotogrammi.

Soluzione

La qualità dell'immagine dipende dalla larghezza di banda della chiamata. Se si aumenta la velocità in bit, migliora la qualità del video, ma sono necessarie risorse di rete aggiuntive. Usare sempre la velocità in bit più adatta al tipo di video. Una videochiamata di 720p e 15 fotogrammi al secondo richiede una velocità in bit di 790 kbps o superiore. Una videochiamata di 720p e 30 fotogrammi al secondo richiede una velocità in bit di 1360 kbps o superiore.

Per ulteriori informazioni sulla larghezza di banda, vedere la sezione Impostazione della risoluzione di trasmissione del video del capitolo "Configurazione e funzioni del telefono".

Soluzione

Verificare che il parametro Velocità in bit di sessione massima per videochiamate sia configurato in modo da essere almeno pari all'intervallo della velocità in bit video minimo. Su Cisco Unified Communications Manager, selezionare **Sistema** > **Informazioni su regione** > **Regione**.

Impossibile trasferire una videochiamata

Problema

Impossibile trasferire una videochiamata dal telefono fisso al dispositivo mobile.

Soluzione

Cisco Unified Mobility non è in grado di gestire le videochiamate. Non è possibile rispondere con il cellulare a una videochiamata ricevuta sul telefono fisso.

Video non disponibile durante una chiamata in conferenza

Problema

Una videochiamata diventa una chiamata audio quando si aggiungono due o più persone alla chiamata.

È necessario utilizzare un video conference bridge per soddisfare esigenze specifiche di videoconferenza automatica.

Problemi generici relativi alle chiamate

Nelle sezioni seguenti vengono fornite delle informazioni per la risoluzione dei problemi generici relativi alle chiamate.

Impossibile stabilire una chiamata

Problema

Un utente ha segnalato l'impossibilità di effettuare una chiamata.

Causa

Sul telefono non è presente un indirizzo IP DHCP; il telefono non è in grado di registrarsi su Cisco Unified Communications Manager. Sui telefoni dotati di display LCD viene visualizzato il messaggio `Configurazione IP` o `Registrazione`. Sui telefoni non dotati di display LCD, quando l'utente tenta di effettuare una chiamata viene riprodotto sul ricevitore il tono di riordino (al posto del segnale di linea).

Soluzione

1. Verificare quanto segue:
    1. Il cavo Ethernet è collegato.
    2. Il servizio Cisco CallManager è in esecuzione sul server Cisco Unified Communications Manager.
    3. Entrambi i telefoni sono registrati sullo stesso server Cisco Unified Communications Manager.
2. I registri di debug e acquisizione del server audio sono abilitati per entrambi i telefoni. Se necessario, abilitare il debug Java.

Le cifre DTMF non vengono riconosciute dal telefono o vengono visualizzate in ritardo

Problema

L'utente ha segnalato che i numeri vengono visualizzati in ritardo o non compaiono quando è in uso la tastiera.

Causa

Se i tasti vengono premuti troppo rapidamente, le cifre potrebbero venire visualizzate in ritardo o non comparire.

Soluzione

Non premere i tasti rapidamente.

Procedure di risoluzione dei problemi

È possibile utilizzare queste procedure per identificare e risolvere i problemi.

Creazione di un rapporto sul problema del telefono in Cisco Unified Communications Manager

È possibile generare un rapporto sul problema per i telefoni in Cisco Unified Communications Manager. Questa azione determina le stesse informazioni generate dal softkey PRT (Problem Report Tool) sul telefono.

Il rapporto sul problema contiene informazioni sul telefono e sulle cuffie.

Procedura

Passaggio 1 In Cisco Unified CM Administration, selezionare **Dispositivo** > **Telefono**.

Passaggio 2 Fare clic su **Trova** e selezionare uno o più telefoni IP Cisco.

Passaggio 3 Fare clic su **Genera PRT per selezionato** per raccogliere i registri PRT per le cuffie utilizzate sui telefoni IP Cisco selezionati.

Creazione di un registro della console dal telefono

Un registro della console viene generato quando il telefono non si connette alla rete e non è possibile accedere allo strumento Segnalazione problemi (PRT).

Prima di iniziare

Collegare un cavo della console alla porta ausiliaria sul retro del telefono.

Procedura

Passaggio 1 Sul telefono, premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Porta AUX**.

Passaggio 3 Selezionare **Raccogli registro console** per raccogliere i registri dei dispositivi.

Verifica delle impostazioni TFTP

Procedura

Passaggio 1 Sul telefono IP Cisco, premere **Applicazioni**, scegliere **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione Ethernet** > **Impostazione IPv4** > **Server TFTP 1**.

Passaggio 2 Se è stato assegnato un indirizzo IP statico al telefono, è necessario immettere manualmente un'impostazione per l'opzione Server TFTP 1.

Passaggio 3 Se si sta utilizzando il protocollo DHCP, il telefono ottiene l'indirizzo del server TFTP dal server DHCP. Verificare che l'indirizzo IP sia configurato nell'opzione 150.

Passaggio 4 È possibile inoltre abilitare il telefono per l'uso di un server TFTP alternativo. Questa impostazione è particolarmente utile se il telefono è stato recentemente spostato da una posizione a un'altra.

Passaggio 5 Se il DHCP locale non fornisce l'indirizzo TFTP corretto, abilitare il telefono per l'uso di un server TFTP alternativo.

Questa impostazione è spesso necessaria negli scenari VPN.

Individuazione dei problemi di connettività o con il DNS

Procedura

Passaggio 1 Utilizzare il menu Reimposta impostazioni per reimpostare le impostazioni del telefono ai valori predefiniti.

Passaggio 2 Modificare le impostazioni DHCP e IP:

a) Disabilitare DHCP.
b) Assegnare dei valori IP statici al telefono. Utilizzare la stessa impostazione del router predefinito configurata su altri telefoni funzionanti.
c) Assegnare un server TFTP. Utilizzare lo stesso server TFTP in uso su altri telefoni funzionanti.

Passaggio 3 Sul server di Cisco Unified Communications Manager, verificare che il nome corretto del server di Cisco Unified Communications Manager riportato nei file host locali sia stato mappato sull'indirizzo IP corretto.

Passaggio 4 Da Cisco Unified Communications Manager, selezionare **Sistema** > **Server** e verificare che l'indirizzo IP (e non il nome DNS) faccia riferimento al server.

Passaggio 5 Da Cisco Unified Communications Manager, selezionare **Dispositivo** > **Telefono**. Fare clic su **Trova** per cercare il telefono. Assicurarsi di aver assegnato l'indirizzo MAC corretto al telefono IP Cisco in uso.

Passaggio 6 Spegnere e riaccendere il telefono.

Argomenti correlati

Reimpostazione di base, a pagina 277
Individuazione dell'indirizzo MAC del telefono, a pagina 72

Verifica delle impostazioni DHCP

Procedura

Passaggio 1 Sul telefono, premere **Applicazioni**  .

Passaggio 2 Selezionare **Wi-Fi** > **Impostazione rete** > **Impostazione IPv4** e osservare le opzioni seguenti:

- Server DHCP: se è stato assegnato un indirizzo IP statico al telefono, non è necessario immettere un valore per l'opzione Server DHCP. Tuttavia, se si sta utilizzando un server DHCP, occorre specificare un valore per questa opzione. Se non viene trovato nessun valore, controllare la configurazione di routing IP e VLAN. Consultare il documento *Risoluzione dei problemi relativi alla porta dello switch e all'interfaccia*, disponibile all'URL seguente:

  http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

- Indirizzo IP, Subnet mask, Router predefinito: se è stato assegnato un indirizzo IP statico al telefono, è necessario immettere manualmente le impostazioni per queste opzioni.

Passaggio 3 Se si sta utilizzando il protocollo DHCP, selezionare gli indirizzi IP distribuiti dal server DHCP.

Consultare il documento *Informazioni e risoluzione dei problemi di DHCP nello switch Catalyst o sulle reti aziendali*, disponibile all'URL seguente:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml.

Creazione di un nuovo file di configurazione del telefono

Se un telefono viene rimosso dal database di Cisco Unified Communications Manager, il file di configurazione viene eliminato dal server TFTP di Cisco Unified Communications Manager. I numeri di rubrica del telefono rimangono nel database di Cisco Unified Communications Manager. Vengono denominati come numeri di rubrica non assegnati ed è possibile utilizzarli per altri dispositivi. Se i numeri di rubrica non assegnati non vengono utilizzati da altri dispositivi, eliminarli dal database di Cisco Unified Communications Manager. È possibile utilizzare il report del piano di indirizzamento per visualizzare ed eliminare i numeri senza alcun riferimento assegnato. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Se vengono modificati i pulsanti di un modello pulsanti del telefono o se a un telefono viene assegnato un modello pulsanti del telefono diverso, i numeri di rubrica non saranno più accessibili dal telefono. Questi numeri vengono comunque assegnati al telefono nel database di Cisco Unified Communications Manager, ma sul telefono non è disponibile nessun pulsante da utilizzare per rispondere alle chiamate. È consigliabile rimuovere tali numeri di rubrica dal telefono ed eliminarli se necessario.

Procedura

Passaggio 1 In Cisco Unified Communications Manager, selezionare **Dispositivo** > **Telefono** e fare clic su **Trova** per individuare il telefono su cui si sta verificando il problema.

Passaggio 2 Selezionare **Elimina** per rimuovere il telefono dal database di Cisco Unified Communications Manager.

Nota Se un telefono viene rimosso dal database di Cisco Unified Communications Manager, il file di configurazione viene eliminato dal server TFTP di Cisco Unified Communications Manager. I numeri di rubrica del telefono rimangono nel database di Cisco Unified Communications Manager. Vengono denominati come numeri di rubrica non assegnati ed è possibile utilizzarli per altri dispositivi. Se i numeri di rubrica non assegnati non vengono utilizzati da altri dispositivi, eliminarli dal database di Cisco Unified Communications Manager. È possibile utilizzare il report del piano di indirizzamento per visualizzare ed eliminare i numeri senza alcun riferimento assegnato.

Passaggio 3 Aggiungere nuovamente il telefono al database di Cisco Unified Communications Manager.

Passaggio 4 Spegnere e riaccendere il telefono.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv
Metodi di aggiunta del telefono, a pagina 73

Identificazione dei problemi di autenticazione 802.1X

Procedura

Passaggio 1 Verificare di aver configurato correttamente i componenti richiesti.

Passaggio 2 Confermare che il segreto condiviso sia configurato sul telefono.

- Se il segreto condiviso è configurato, verificare che sul server di autenticazione sia presente lo stesso segreto condiviso.
- Se il segreto condiviso non è configurato sul telefono, immetterlo e assicurarsi che corrisponda a quello configurato sul server di autenticazione.

Verifica delle impostazioni DNS

Per verificare le impostazioni DNS, attenersi alla procedura seguente:

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Impostazione di rete** > **Impostazione IPv4** > **Server DNS 1**.

Passaggio 3 È necessario inoltre verificare che sia stata immessa una voce CNAME nel server DNS per il server TFTP e per il sistema Cisco Unified Communications Manager.

Occorre inoltre assicurarsi che il DNS sia configurato per l'esecuzione delle ricerche inverse.

Avvio del servizio

Prima di avviare o arrestare un servizio, è necessario attivarlo.

Procedura

Passaggio 1 Da Cisco Unified Communications Manager Administration, selezionare **Cisco Unified Serviceability** dall'elenco a discesa Navigazione e fare clic su **Vai**.

Passaggio 2 Selezionare **Strumenti** > **Centro di controllo - Servizi funzioni**.

Passaggio 3 Selezionare il server primario di Cisco Unified Communications Manager dall'elenco a discesa Server.

Nella finestra vengono visualizzati i nomi dei servizi del server selezionato, il relativo stato e un pannello di controllo del servizio tramite cui avviarlo o arrestarlo.

Passaggio 4 Se un servizio è stato arrestato, fare clic sul pulsante di opzione corrispondente, quindi su **Avvia**.

Il simbolo dello stato del servizio cambia da un quadrato in una freccia.

Controllo delle informazioni di debug da Cisco Unified Communications Manager

Se sul telefono si verificano dei problemi che non si è in grado di risolvere, è possibile richiedere assistenza a Cisco TAC. È necessario attivare il debug per il telefono, riprodurre il problema, disattivare il debug e inviare i registri a TAC per l'analisi.

Dal momento che tramite il debug vengono acquisite delle informazioni dettagliate, il traffico della comunicazione potrebbe rallentare le prestazioni del telefono, rendendolo meno reattivo. In seguito all'acquisizione dei registri, disattivare il debug per garantire il corretto funzionamento del telefono.

Le informazioni di debug possono includere un codice a una cifra indicante il livello di gravità della situazione. Le situazioni vengono classificate come segue:

- 0: Emergenza
- 1: Allarme
- 2: Critico
- 3: Errore
- 4: Avviso
- 5: Notifica
- 6: Informazioni
- 7: Debug

Contattare Cisco TAC per ulteriori informazioni e assistenza.

Procedura

Passaggio 1 In Cisco Unified Communications Manager Administration, selezionare una delle finestre seguenti:

- **Dispositivo** > **Impostazioni dispositivo** > **Profilo telefono comune**
- **Sistema** > **Configurazione telefono aziendale**
- **Dispositivo** > **Telefono**

Passaggio 2 Impostare i parametri seguenti:

- Profilo registro - valori: Predefinito (impostazione predefinita), Valore predefinito, Telefonia, SIP, UI, Rete, Media, Aggiornamento, Accessorio, Sicurezza, Wi-Fi, VPN, EnergyWise, MobileRemoteAccess

  Nota Per implementare il supporto multilivello e multisessione dei parametri, selezionare la casella di controllo Profilo registro.

- Registro remoto - valori: Disabilita (impostazione predefinita), Abilita
- Server di registro IPv6 o Server di registro: Indirizzo IP (indirizzi IPv4 o IPv6)

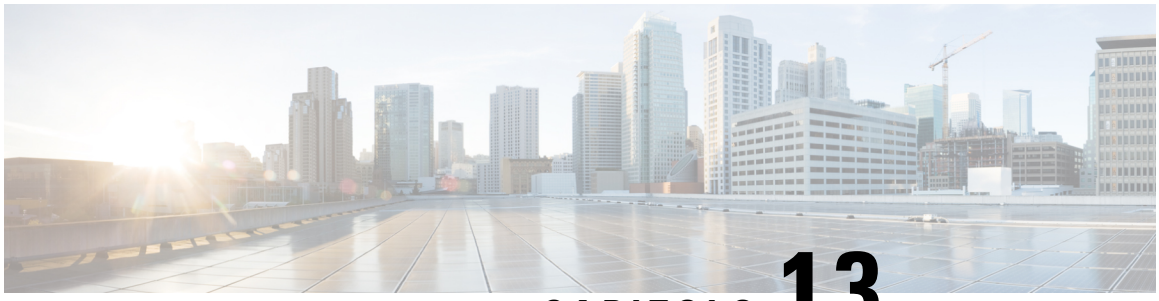
Nota Se non è possibile raggiungere il server di registro, il telefono arresta l'invio dei messaggi di debug.

- Il formato dell'indirizzo del server di registro IPv4 è **indirizzo:<port>@@base=<0-7>;pfs=<0-1>**
- Il formato dell'indirizzo del server di registro IPv6 è **[indirizzo]:<port>@@base=<0-7>;pfs=<0-1>**
- Dove:
  - l'indirizzo IPv4 è separato con un punto (.)
  - l'indirizzo IPv6 è separato con i due punti (:)

Informazioni aggiuntive sulla risoluzione dei problemi

In caso di domande aggiuntive sulla risoluzione dei problemi relativi al telefono, accedere al sito Web di Cisco riportato di seguito e navigare fino al modello del telefono desiderato:

https://www.cisco.com/cisco/web/psa/troubleshoot.html



CAPITOLO 13

Manutenzione

Reimpostazione di base

Tramite la reimpostazione di base di un telefono IP Cisco, è possibile riprendere l'esecuzione del telefono in caso di errore e reimpostare o ripristinare diverse impostazioni di configurazione e sicurezza.

Nella tabella seguente vengono illustrate le diverse modalità di esecuzione di una reimpostazione di base. È possibile reimpostare il telefono, dopo averlo avviato, tramite una delle seguenti operazioni. Scegliere l'operazione più adatta alle proprie esigenze.

Tabella 54: Metodi di reimpostazione di base

Operazione	Azione	Spieg
Riavvio del telefono	Premere **Applicazioni**. Accedere a **Impostazioni amministratore** > **Reimposta impostazioni** > **Reimposta dispositivo**.	Ripri confi riavv
Reimpostazione delle impostazioni	Per reimpostare le impostazioni, premere **Applicazioni** e selezionare **Impostazioni amministratore** > **Reimposta applicazioni** > **Rete**.	Reim
	Per reimpostare il file CTL, premere **Applicazioni** e selezionare **Impostazioni amministratore** > **Reimposta impostazioni** > **Protezione**.	Reim

Reimpostazione del telefono alle impostazioni predefinite dalla tastiera

È possibile reimpostare il telefono alle impostazioni predefinite. La reimpostazione cancella tutti i parametri del telefono.

Procedura

Passaggio 1 Rimuovere l'alimentazione dal telefono in uno dei modi seguenti:

- Scollegare l'alimentatore.
- Scollegare il cavo LAN.

Passaggio 2 Attendere 5 secondi.

Passaggio 3 Premere e tenere premuto **#** e ricollegare il telefono. Rilasciare il tasto **#** solo quando i tasti **Cuffia** e **Altoparlante** sono accesi.

Nota In alcune versioni hardware, il pulsante **Disattiva audio** si accende anche con i tasti **Cuffia** e **Altoparlante** quando si collega nuovamente il telefono. In questo caso, attendere che tutte le parti vengano rilasciate e rilasciare il tasto **#** solo quando i tasti **Cuffia** e **Altoparlante** sono di nuovo accesi.

Passaggio 4 Immettere la seguente sequenza di tasti:

```
123456789*0#
```

La spia del pulsante **Cuffia** si spegne dopo aver premuto il tasto **1**. Dopo aver immesso la sequenza di tasti, il pulsante **Disattiva audio** si illumina.

Attenzione Non spegnere il telefono fino al completamento della procedura di ripristino e fino alla visualizzazione della schermata principale.

Il telefono viene reimpostato.

Esecuzione della funzione Reimposta tutte le impostazioni dal menu del telefono

Eseguire questa attività se si desidera ripristinare i valori predefiniti delle impostazioni dell'utente e della configurazione di rete.

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Impostazioni amministratore** > **Reimposta impostazioni** > **Tutte le impostazioni**.

Se necessario, sbloccare le opzioni del telefono.

Riavvio del telefono dall'immagine di backup

Il telefono IP Cisco dispone di una seconda immagine di backup che consente di ripristinare il telefono quando è stata compromessa l'immagine predefinita.

Per riavviare il telefono dall'immagine di backup, attenersi alla seguente procedura.

Procedura

Passaggio 1	Scollegare l'alimentatore.
Passaggio 2	Tenere premuto il tasto asterisco (*).
Passaggio 3	Ricollegare l'alimentatore. Continuare a tenere premuto il tasto asterisco fino a quando non si spegne il LED del pulsante DisatMic.
Passaggio 4	Rilasciare il tasto asterisco. Il telefono viene riavviato dall'immagine di backup.

Esecuzione della reimpostazione della configurazione di rete

Reimposta le impostazioni di configurazione di rete ai valori predefiniti e riavvia il telefono. Questo metodo comporta la riconfigurazione dell'indirizzo IP del telefono da parte di DHCP.

Procedura

Passaggio 1	Dal menu Impostazioni amministratore, se necessario, sbloccare le opzioni del telefono.
Passaggio 2	Selezionare **Reimposta impostazioni** > **Impostazione di rete**.

Esecuzione della reimpostazione della configurazione di rete dell'utente

Reimposta alle impostazioni salvate in precedenza le modifiche apportate alla configurazione della rete o dell'utente, ma che il telefono non ha scritto nella memoria flash.

Procedura

Passaggio 1	Dal menu Impostazioni amministratore, se necessario, sbloccare le opzioni del telefono.
Passaggio 2	Selezionare **Reimposta impostazioni** > **Reimposta dispositivo**.

Rimozione di un file CTL

Elimina soltanto il file CTL dal telefono.

Procedura

Passaggio 1	Dal menu Impostazioni amministratore, se necessario, sbloccare le opzioni del telefono.
Passaggio 2	Selezionare **Reimposta impostazioni** > **Impostazioni di protezione**.

Quality Report Tool

Il Quality Report Tool (QRT) è uno strumento per il controllo della qualità audio e per la segnalazione di problemi generali relativi al telefono IP Cisco. La funzione dello strumento QRT è disponibile come parte dell'installazione di Cisco Unified Communications Manager.

È possibile configurare lo strumento QRT sui telefoni IP Cisco degli utenti. In questo modo, questi ultimi potranno segnalare gli eventuali problemi relativi alle chiamate premendo Rapporto qualità. Questo softkey o pulsante è disponibile soltanto se il telefono IP Cisco si trova nello stato Connesso, Connected Conference, Connected Transfer o Ricevitore agganciato.

Quando un utente preme Rapporto qualità, viene visualizzato un elenco delle categorie dei problemi. L'utente seleziona la categoria del problema appropriata e il feedback viene registrato in un file XML. Le informazioni che vengono effettivamente registrate dipendono dalla selezione effettuata dall'utente e dal fatto che il dispositivo di destinazione sia un telefono IP Cisco.

Per ulteriori informazioni sull'uso dello strumento QRT, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Monitoraggio della qualità audio

Per misurare la qualità vocale delle chiamate inviate e ricevute nella rete, i telefoni IP di Cisco utilizzano le seguenti metriche statistiche basate su eventi di occultamento. Il DSP riproduce i frame di occultamento per mascherare la perdita di frame nel flusso del pacchetto voce.

- Metriche indice occultamento: mostrano l'indice dei frame di occultamento rispetto al totale dei frame voce. Gli indici occultamento intervallo vengono calcolati ogni 3 secondi.
- Metriche secondi occultamento: mostrano il numero di secondi in cui il DSP riproduce i frame di occultamento a causa dei frame persi. Un «secondo occultamento» rigoroso è un secondo in cui il DSP riproduce più del cinque percento dei frame di occultamento.

Nota L'indice di occultamento e i secondi di occultamento sono delle misurazioni primarie basate sulla perdita di frame. Un indice di occultamento pari a zero indica che i frame e i pacchetti vengono consegnati in orario e senza nessuna perdita sulla rete IP.

È possibile accedere alle metriche sulla qualità audio dalla schermata Statistiche chiamate del telefono IP Cisco o da remoto mediante Statistiche di flusso.

Suggerimenti per la risoluzione dei problemi relativi alla qualità audio

Se si notano delle modifiche significative e ripetute alle metriche, fare riferimento alla tabella seguente per delle informazioni generali sulla risoluzione dei problemi.

Tabella 55: Modifiche delle metriche della qualità audio

Modifica della metrica	Condizione
Aumento significativo dell'indice e dei secondi di occultamento	Problema di rete derivante dalla perdita di pacchetti o da jitter elevato.
L'indice di occultamento è vicino o pari a zero, ma la qualità audio è scarsa.	• Rumori o distorsioni, come ad esempio eco o livelli audio, all'interno del canale audio. • Per le chiamate in parallelo si verificano più eventi di codifica/decodifica, come ad esempio per le chiamate a una rete cellulare o a una rete con carta telefonica. • Problemi acustici derivanti da altoparlanti, sistema vivavoce per cellulari o cuffie wireless. Controllare il numero di pacchetti trasmessi (TxCnt) e ricevuti (RxCnt) per verificare che non sia presente alcun problema nel flusso dei pacchetti voce.
Diminuzione significativa dei punteggi MOS LQK	Problema di rete derivante dalla perdita di pacchetti o da livelli di jitter elevati: • La diminuzione dei punteggi MOS LQK medi può indicare un problema uniforme e diffuso in tutto il sistema. • La diminuzione del punteggio MOS LQK individuale può indicare un problema già in corso. Controllare l'indice e i secondi di occultamento per verificare se è in corso la perdita di pacchetti e se si è registrato un livello di jitter elevato.
Aumento significativo dei punteggi MOS LQK	• Verificare se il telefono sta utilizzando un codec diverso da quello previsto (RxType e TxType). • Verificare se la versione MOS LQK è cambiata in seguito all'aggiornamento del firmware.

Nota Nelle metriche sulla qualità audio non vengono presi in considerazione i rumori o le distorsioni, ma solo la perdita di frame.

Pulizia del telefono IP Cisco

Per pulire il telefono IP Cisco, utilizzare esclusivamente un panno morbido e asciutto da passare delicatamente sul telefono e sullo schermo. Non applicare sostanze liquide o in polvere direttamente sul telefono. Come per tutti i dispositivi non impermeabili, le sostanze liquide e in polvere possono danneggiare i componenti e causare guasti.

Quando il telefono è in modalità di risparmio energetico, lo schermo si disattiva e il pulsante Seleziona è spento. Quando il telefono è in questo stato, è possibile pulire lo schermo, purché sia noto che il telefono resterà disattivato fino a quando la pulizia non sia terminata.

CAPITOLO 14

Supporto utente internazionale

Programma di configurazione delle impostazioni internazionali per gli endpoint di Unified Communications Manager

Per impostazione predefinita, i telefoni IP Cisco sono configurati sulle impostazioni internazionali per l'inglese (Stati Uniti). Per utilizzare i telefoni IP Cisco con altre versioni delle impostazioni internazionali, occorre installare su ciascun server di Cisco Unified Communications Manager presente nel cluster la versione del programma di configurazione delle impostazioni internazionali degli endpoint di Cisco Unified Communications Manager. Il programma di installazione delle impostazioni internazionali installa sul sistema la traduzione più recente del testo dell'interfaccia utente del telefono e le suonerie specifiche del Paese in modo di renderle disponibili per i telefoni IP Cisco.

Per accedere al programma di configurazione delle impostazioni internazionali richiesto per una versione, accedere alla pagina Download software, navigare fino al modello di telefono in uso e selezionare il collegamento al programma di configurazione delle impostazioni internazionali per gli endpoint di Unified Communications Manager.

Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Nota La versione più recente del programma di configurazione delle impostazioni internazionali potrebbe non essere immediatamente disponibile; controllare frequentemente il sito Web per gli aggiornamenti.

Argomenti correlati

Documentazione di Cisco Unified Communications Manager, a pagina xv

Supporto per la registrazione delle chiamate internazionali

Se il sistema del telefono è configurato per la registrazione delle chiamate internazionali (normalizzazione della parte chiamante), nelle voci dei registri delle chiamate, dell'elenco di ricomposizione o della rubrica è possibile visualizzare un simbolo più (+) che rappresenta il codice di escape internazionale relativo alla propria posizione. A seconda della configurazione del sistema del telefono, il simbolo + potrebbe essere sostituito con il codice di composizione internazionale corretto oppure potrebbe essere necessario modificare il numero prima di comporlo per sostituire manualmente il simbolo + con il codice di escape internazionale relativo alla propria posizione. Inoltre, mentre nella voce del registro chiamate o della rubrica è possibile visualizzare il numero internazionale completo per la chiamata ricevuta, nel display del telefono potrebbe venire invece visualizzata la versione locale abbreviata del numero, senza codici internazionali o del Paese.

Limitazione di lingua

Non è supportata l'immissione di testo alfanumerico da tastiera per le seguenti impostazioni internazionali asiatiche:

- Cinese (Hong Kong)
- Cinese (Taiwan)
- Giapponese (Giappone)
- Coreano (Corea del Sud)

All'utente viene proposta l'immissione di testo alfanumerico da tastiera predefinita in inglese (Stati Uniti).

Ad esempio, sullo schermo del telefono viene visualizzato il testo in coreano, ma sul tasto **2** delle tastiera è riportato **a b c 2 A B C**.

L'immissione di testo in cinese funziona in modo analogo ai PC e ai telefoni cellulari in cinese. Per il corretto funzionamento dell'immissione di testo in cinese, è necessario il programma di configurazione delle impostazioni per la lingua cinese.