



Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per Cisco Unified Communications Manager

Prima pubblicazione: 2017-09-15

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 QUI 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 COMMERCIALIZZABILITÀ, 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, CONSEGUENZIALI 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2023 Cisco Systems, Inc. Tutti i diritti riservati.



SOMMARIO

CAPITOLO 1

Novità e modifiche 1

Novità e modifiche per la versione del firmware 14.2(1)	1
Novità e modifiche per la versione del firmware 14.1(1)	1
Novità e modifiche per la versione del firmware 14.0(1)	2
Novità e modifiche per la versione del firmware 12.8(1)	2
Novità e modifiche per la versione del firmware 12.7(1)	2
Novità e modifiche per la versione del firmware 12.6(1)	2
Novità e modifiche per la versione del firmware 12.5(1)SR3	3
Novità e modifiche per la versione del firmware 12.5(1)SR2	3
Novità e modifiche per la versione del firmware 12.5(1)SR1	3
Novità e modifiche per la versione del firmware 12.5(1)	3
Novità e modifiche per la versione del firmware 12.1(1)	4

PARTE I:

Informazioni sul telefono IP per chiamate in conferenza Cisco 7

CAPITOLO 2

Hardware del telefono IP per chiamate in conferenza Cisco 9

Telefono IP per chiamate in conferenza Cisco 8832	9
Pulsanti e hardware del telefono IP per chiamate in conferenza Cisco 8832	11
Microfono di espansione con cavo (solo 8832)	12
Microfono di espansione wireless (solo 8832)	13
Documentazione correlata	14
Documentazione del telefono IP per chiamate in conferenza Cisco 8832	14
Documentazione di Cisco Unified Communications Manager	14
Documentazione di Cisco Unified Communications Manager Express	15
Documentazione di Cisco HCS (Hosted Collaboration Service)	15
Documentazione di Cisco Business Edition 4000	15

Documentazione, supporto e linee guida di sicurezza	15
Informazioni generali sulla protezione del prodotto Cisco	15
Differenze terminologiche	16

CAPITOLO 3**Dettagli tecnici 17**

Specifiche fisiche e dell'ambiente operativo	17
Requisiti di alimentazione dei telefoni	18
Interruzione dell'alimentazione	19
Consumi energetici ridotti	19
Protocolli di rete	20
Interazione con Cisco Unified Communications Manager	22
Interazione con Cisco Unified Communications Manager Express	23
Interazione con il sistema di voice messaging	23
File di configurazione del telefono	24
Comportamento del telefono durante le ore di congestione della rete	24
Application Programming Interface	25

PARTE II:**Installazione del telefono IP per chiamate in conferenza Cisco 27****CAPITOLO 4****Installazione del telefono 29**

Verifica dell'impostazione di rete	29
Onboarding tramite codice di attivazione per telefoni in sede	30
Onboarding tramite codice di attivazione e accesso mobile e remoto	31
Abilitazione della registrazione automatica sul telefono	31
Modalità collegamento a cascata	33
Installazione del telefono per chiamate in conferenza	33
Modalità di alimentazione del telefono per chiamate in conferenza	35
Installazione di microfoni di espansione con cavo	37
Installazione dei microfoni di espansione wireless	38
Installazione della base di caricamento per microfono wireless	39
Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata	40
Riavvio del telefono per chiamate in conferenza dall'immagine di backup	41
Impostazione del telefono dai menu di configurazione	42
Applicazione di una password al telefono	43

Voci di menu e di testo del telefono	43
Configurazione delle impostazioni di rete	44
Campi di Impostazione di rete	44
Impostazione del campo Nome dominio	49
Abilitazione della LAN wireless dal telefono	49
Impostazione della LAN wireless da Cisco Unified Communications Manager	50
Impostazione della LAN wireless dal telefono	50
Impostazione del numero di tentativi di autenticazione WLAN	52
Abilitazione della modalità prompt WLAN	53
Impostazione di un profilo Wi-Fi utilizzando Cisco Unified Communications Manager	53
Impostazione di un gruppo Wi-Fi utilizzando Cisco Unified Communications Manager	55
Verifica dell'avvio del telefono	55
Modifica del modello del telefono di un utente	56

CAPITOLO 5 **Installazione del telefono su Cisco Unified Communications Manager** 57

Impostazione di un telefono IP per chiamate in conferenza Cisco	57
Individuazione dell'indirizzo MAC del telefono	62
Metodi di aggiunta del telefono	62
Aggiunta di singoli telefoni	62
Aggiunta di telefoni con modello telefono BAT	63
Aggiunta degli utenti a Cisco Unified Communications Manager	63
Aggiunta di un utente da una rubrica LDAP esterna	64
Aggiunta di un utente direttamente a Cisco Unified Communications Manager	64
Aggiunta di un utente a un gruppo di utenti finali	65
Associazione dei telefoni agli utenti	66
SRST (Survivable Remote Site Telephony)	66

CAPITOLO 6 **Gestione del portale Self Care** 69

Panoramica del portale Self Care	69
Impostazione dell'accesso degli utenti al portale Self Care	69
Personalizzazione della visualizzazione del portale Self Care	70

PARTE III: **Amministrazione del telefono IP per chiamate in conferenza Cisco** 71

CAPITOLO 7	Sicurezza del telefono IP per chiamate in conferenza Cisco	73
	Panoramica sulla protezione del telefono IP Cisco	73
	Miglioramento della protezione della rete telefonica	74
	Funzioni di protezione supportate	75
	Impostazione di un LSC (Locally Significant Certificate)	77
	Abilitazione della modalità FIPS	79
	Protezione delle chiamate	79
	Identificazione delle chiamate in conferenza protette	80
	Identificazione delle chiamate protette	81
	Fornitura della crittografia per l'Inclusione	82
	Protezione WLAN	82
	Protezione LAN wireless	85
	Pagina Amministrazione del telefono IP Cisco	85
	Configurazione SCEP	88
	Autenticazione 802.1x	89
CAPITOLO 8	Personalizzazione del telefono IP per chiamate in conferenza Cisco	91
	Suonerie personalizzate del telefono	91
	Impostazione di una suoneria personalizzata	91
	Formati di file delle suonerie personalizzate	92
	Personalizzazione del segnale di linea	93
CAPITOLO 9	Funzioni e impostazione del telefono IP per chiamate in conferenza Cisco	95
	Supporto utente per il telefono IP Cisco	95
	Migrazione diretta del telefono a un telefono multiplatforma	95
	Impostazione di un nuovo modello di softkey	96
	Configurazione dei servizi telefonici per gli utenti	97
	Configurazione delle funzioni del telefono	97
	Impostazione delle funzioni del telefono per tutti i telefoni	98
	Impostazione delle funzioni del telefono per un gruppo di telefoni	98
	Impostazione delle funzioni del telefono per un telefono singolo	99
	Configurazione specifica del prodotto	99
	Disabilitazione delle crittografie TLS (Transport Layer Security)	112

	Pianificazione della modalità Risparmio energia per il telefono IP Cisco	113
	Pianificazione di EnergyWise sul telefono IP Cisco	114
	Impostazione dell'opzione Non disturbare	118
	Impostazione delle notifiche di deviazione chiamate	118
	Impostazione del parametro UCR 2008	119
	Impostazione del parametro UCR 2008 in Configurazione dispositivo comune	120
	Impostazione del parametro UCR 2008 in Profilo telefono comune	120
	Impostazione del parametro UCR 2008 in Configurazione telefono aziendale	121
	Impostazione del parametro UCR 2008 in Telefono	121
	Mobile and Remote Access Through Expressway	121
	Scenari di distribuzione	123
	Configurazione di credenziali utente persistenti per l'accesso a Expressway	123
	Problem Reporting Tool (PRT)	124
	Configurazione di un URL di caricamento assistenza clienti	124
	Impostazione di un'etichetta per una linea	125
<hr/>		
CAPITOLO 10	Rubrica aziendale ed Elenco personale	127
	Impostazione della rubrica aziendale	127
	Impostazione dell'Elenco personale	127
<hr/>		
PARTE IV:	Risoluzione dei problemi del telefono IP per chiamate in conferenza Cisco	129
<hr/>		
CAPITOLO 11	Monitoraggio dei sistemi telefonici	131
	Panoramica sul monitoraggio dei sistemi telefonici	131
	Stato del telefono IP Cisco	131
	Visualizzazione della finestra Informazioni telefono	132
	Visualizzazione del menu Stato	132
	Visualizzazione della finestra Messaggi di stato	132
	Visualizzazione della finestra Statistiche di rete	137
	Visualizzazione della finestra Statistiche chiamate	140
	Pagina Web del telefono IP Cisco	142
	Accesso alla pagina Web del telefono	142
	Pagina Web Informazioni dispositivo	142
	Pagina Web Impostazioni di rete	144

Pagina Web Informazioni Ethernet	148
Pagine Web Rete	149
Pagine Web Registri console, Dump della memoria, Messaggi di stato e Visualizzazione debug	150
Pagina Web Statistiche di flusso	151
Richiesta di informazioni dal telefono in formato XML	153
Output CallInfo di esempio	154
Output LineInfo di esempio	154
Output ModeInfo di esempio	155

CAPITOLO 12
Risoluzione dei problemi del telefono 157

Informazioni generali sulla risoluzione dei problemi	157
Problemi di avvio	158
Il telefono IP Cisco non segue la normale procedura di avvio	159
Impossibile effettuare la registrazione del telefono IP Cisco su Cisco Unified Communications Manager	159
Il telefono visualizza messaggi di errore	160
Il telefono non è in grado di connettersi al server TFTP o a Cisco Unified Communications Manager	160
Il telefono non è in grado di connettersi al server TFTP	160
Il telefono non è in grado di connettersi al server	160
Il telefono non è in grado di connettersi tramite DNS	161
Mancata esecuzione di Cisco Unified Communications Manager e dei servizi TFTP	161
File di configurazione danneggiato	161
Registrazione del telefono su Cisco Unified Communications Manager	162
Impossibile ottenere l'indirizzo IP sul telefono IP Cisco	162
Problemi di reimpostazione del telefono	162
Il telefono si reimposta a causa di interruzioni di rete a intermittenza	163
Il telefono viene reimpostato a causa di errori dell'impostazione DHCP	163
Il telefono si reimposta a causa di un indirizzo IP statico errato	163
Il telefono si reimposta durante l'uso intenso della rete	163
Il telefono si reimposta a causa di una reimpostazione volontaria	164
Il telefono si reimposta a causa di problemi con il DNS o di altri problemi di connettività	164
Il telefono non si accende	164
Il telefono non è in grado di connettersi alla LAN	165

Problemi di protezione del telefono IP Cisco	165
Problemi relativi al file CTL	165
Errore di autenticazione; il telefono non è in grado di autenticare il file CTL	165
Il telefono non è in grado di autenticare il file CTL	165
È possibile autenticare il file CTL, ma non gli altri file di configurazione	166
È possibile autenticare il file ITL, ma non gli altri file di configurazione	166
Errore di autorizzazione TFTP	166
Impossibile effettuare la registrazione del telefono	167
File di configurazione firmati non richiesti	167
Problemi audio	167
Nessun percorso audio	167
Audio disturbato	167
Un telefono in modalità collegamento a cascata non funziona	168
Problemi generici relativi alle chiamate	168
Impossibile stabilire una chiamata	168
Le cifre DTMF non vengono riconosciute dal telefono o vengono visualizzate in ritardo	169
Procedure di risoluzione dei problemi	169
Creazione di un rapporto sul problema del telefono in Cisco Unified Communications Manager	169
Verifica delle impostazioni TFTP	169
Individuazione dei problemi di connettività o con il DNS	170
Verifica delle impostazioni DHCP	170
Creazione di un nuovo file di configurazione del telefono	171
Verifica delle impostazioni DNS	172
Avvio del servizio	172
Controllo delle informazioni di debug da Cisco Unified Communications Manager	173
Informazioni aggiuntive sulla risoluzione dei problemi	174

CAPITOLO 13**Manutenzione 175**

Riavvio o reimpostazione del telefono per chiamate in conferenza	175
Riavvio del telefono per chiamate in conferenza	175
Reimpostazione delle impostazioni del telefono per chiamate in conferenza dal menu del telefono	175
Ripristino delle impostazioni di fabbrica predefinite del telefono per chiamate in conferenza dalla tastiera	176
Monitoraggio della qualità audio	176

Suggerimenti per la risoluzione dei problemi relativi alla qualità audio 177
Pulizia del telefono IP Cisco 178

CAPITOLO 14

Supporto utente internazionale 179

Programma di configurazione delle impostazioni internazionali per gli endpoint di Unified
Communications Manager 179
Supporto per la registrazione delle chiamate internazionali 180
Limitazione di lingua 180



CAPITOLO 1

Novità e modifiche

- [Novità e modifiche per la versione del firmware 14.2\(1\), a pagina 1](#)
- [Novità e modifiche per la versione del firmware 14.1\(1\), a pagina 1](#)
- [Novità e modifiche per la versione del firmware 14.0\(1\), a pagina 2](#)
- [Novità e modifiche per la versione del firmware 12.8\(1\), a pagina 2](#)
- [Novità e modifiche per la versione del firmware 12.7\(1\), a pagina 2](#)
- [Novità e modifiche per la versione del firmware 12.6\(1\), a pagina 2](#)
- [Novità e modifiche per la versione del firmware 12.5\(1\)SR3, a pagina 3](#)
- [Novità e modifiche per la versione del firmware 12.5\(1\)SR2, a pagina 3](#)
- [Novità e modifiche per la versione del firmware 12.5\(1\)SR1, a pagina 3](#)
- [Novità e modifiche per la versione del firmware 12.5\(1\), a pagina 3](#)
- [Novità e modifiche per la versione del firmware 12.1\(1\), a pagina 4](#)

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 74

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 74
Migrazione del telefono senza caricamento di transizione	Migrazione diretta del telefono a un telefono multiplatforma, a pagina 95

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 99
Miglioramenti a SIP OAuth	Miglioramento della protezione della rete telefonica, a pagina 74
Miglioramenti a OAuth per MRA	Mobile and Remote Access Through Expressway, a pagina 121
Miglioramenti dell'interfaccia utente	SRST (Survivable Remote Site Telephony), a pagina 66

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 56
Aggiunta di ulteriori informazioni sul campo Accesso Web	Configurazione specifica del prodotto, a pagina 99

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

Non è stato necessario aggiornare la Guida all'amministrazione per la versione del firmware 12.7(1).

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

Non è stato necessario aggiornare la Guida all'amministrazione per la versione del firmware 12.6(1).

Novità e modifiche per la versione del firmware 12.5(1)SR3

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

Tabella 2: Revisioni della Guida all'amministrazione del telefono IP Cisco 8832 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 31
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 169

Novità e modifiche per la versione del firmware 12.5(1)SR2

Non è stato necessario aggiornare la Guida all'amministrazione per la versione del firmware 12.5(1)SR2.

La versione del firmware 12.5(1)SR2 sostituisce la versione del firmware 12.5(1) e la versione del firmware 12.5(1)SR1. La versione del firmware 12.5(1) e la versione del firmware 12.5(1)SR1 sono state differite in favore della versione del firmware 12.5(1)SR2.

Novità e modifiche per la versione del firmware 12.5(1)SR1

Nella seguente tabella vengono elencate le modifiche alla *Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per Cisco Unified Communications Manager* per supportare la versione del firmware 12.5(1)SR1.

Tabella 3: Revisioni della Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per la versione del firmware 12.5(1)SR1

Revisione	Sezione nuova o aggiornata
Supporto per crittografia a curva ellittica	Funzioni di protezione supportate, a pagina 75

Novità e modifiche per la versione del firmware 12.5(1)

Nella seguente tabella vengono elencate le modifiche alla *Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per Cisco Unified Communications Manager* per supportare la versione del firmware 12.5(1).

Tabella 4: Revisioni della Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per la versione del firmware 12.5(1)

Revisione	Sezione nuova o aggiornata
Supporto per messaggi privati su Cisco Unified Communications Manager Express	Interazione con Cisco Unified Communications Manager Express, a pagina 23
Supporto per la disabilitazione delle crittografie TLS	Configurazione specifica del prodotto, a pagina 99
Supporto per la composizione Enbloc per il miglioramento del timer di interdigitazione T.302.	Configurazione specifica del prodotto, a pagina 99

Novità e modifiche per la versione del firmware 12.1(1)

Nella seguente tabella vengono descritte le modifiche alla *Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per Cisco Unified Communications Manager* per supportare la versione del firmware 12.1(1).

Revisione	Sezione nuova o aggiornata
Il supporto di Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832	<ul style="list-style-type: none"> • Requisiti di alimentazione dei telefoni, a pagina 18 • Modalità di alimentazione del telefono per chiamate in conferenza, a pagina 35 • Installazione del telefono per chiamate in conferenza, a pagina 33
Supporto per microfoni wireless	<ul style="list-style-type: none"> • Telefono IP per chiamate in conferenza Cisco 8832, a pagina 9 • Microfono di espansione wireless (solo 8832), a pagina 13 • Installazione dei microfoni di espansione wireless, a pagina 38 • Installazione della base di caricamento per microfono wireless, a pagina 39
Supporto per collegamento a cascata	<ul style="list-style-type: none"> • Telefono IP per chiamate in conferenza Cisco 8832, a pagina 9 • Modalità collegamento a cascata, a pagina 33 • Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata, a pagina 40 • Un telefono in modalità collegamento a cascata non funziona, a pagina 168

Revisione	Sezione nuova o aggiornata
Il supporto di Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832	<ul style="list-style-type: none"> • Installazione del telefono per chiamate in conferenza, a pagina 33 • Modalità di alimentazione del telefono per chiamate in conferenza, a pagina 35
Supporto per Wi-Fi	<ul style="list-style-type: none"> • Installazione del telefono per chiamate in conferenza, a pagina 33 • Modalità di alimentazione del telefono per chiamate in conferenza, a pagina 35 • Impostazione del campo Nome dominio, a pagina 49 • Abilitazione della LAN wireless dal telefono, a pagina 49 • Impostazione della LAN wireless da Cisco Unified Communications Manager, a pagina 50 • Impostazione della LAN wireless dal telefono, a pagina 50 • Impostazione del numero di tentativi di autenticazione WLAN, a pagina 52 • Abilitazione della modalità prompt WLAN, a pagina 53 • Impostazione di un profilo Wi-Fi utilizzando Cisco Unified Communications Manager, a pagina 53 • Impostazione di un gruppo Wi-Fi utilizzando Cisco Unified Communications Manager, a pagina 55
Supporto per accesso remoto e mobile tramite Expressway	<ul style="list-style-type: none"> • Mobile and Remote Access Through Expressway, a pagina 121 • Scenari di distribuzione, a pagina 123 • Configurazione di credenziali utente persistenti per l'accesso a Expressway, a pagina 123
Supporto per l'abilitazione o la disabilitazione di TLS 1.2 per l'accesso al server Web	Configurazione specifica del prodotto, a pagina 99
Supporto per codec audio G722.2 AMR-WB	<ul style="list-style-type: none"> • Telefono IP per chiamate in conferenza Cisco 8832, a pagina 9 • Campi di Statistiche chiamate, a pagina 140



PARTE **I**

Informazioni sul telefono IP per chiamate in conferenza Cisco

- [Hardware del telefono IP per chiamate in conferenza Cisco, a pagina 9](#)
- [Dettagli tecnici, a pagina 17](#)



CAPITOLO 2

Hardware del telefono IP per chiamate in conferenza Cisco

- [Telefono IP per chiamate in conferenza Cisco 8832, a pagina 9](#)
- [Pulsanti e hardware del telefono IP per chiamate in conferenza Cisco 8832, a pagina 11](#)
- [Documentazione correlata, a pagina 14](#)
- [Documentazione, supporto e linee guida di sicurezza, a pagina 15](#)
- [Differenze terminologiche, a pagina 16](#)

Telefono IP per chiamate in conferenza Cisco 8832

Cisco IP Conference Phone 8832 e 8832NR migliorano le comunicazioni tra persone unendo prestazioni audio ad alta definizione (HD) superiori e copertura a 360 gradi per tutte le dimensioni di sale riunioni e uffici di responsabili. Questi modelli garantiscono un'esperienza audiofila grazie a un altoparlante full-duplex bidirezionale vivavoce ad ampia banda audio (G.722). Questo telefono è una soluzione semplice che risolve le problematiche legate alle sale più diverse.

Figura 1: Telefono IP per chiamate in conferenza Cisco 8832



Il telefono per chiamate in conferenza dispone di microfoni sensibili con copertura a 360 gradi. Questa copertura consente agli utenti di parlare con voce normale e di essere uditi chiaramente fino a 3 m di distanza. La

tecnologia del telefono è in grado di resistere alle interferenze prodotte da cellulari e altri dispositivi wireless per assicurare la chiarezza delle comunicazioni e l'assenza di distrazioni. Il telefono è dotato di schermo a colori e tasti softkey per accedere alle funzioni utente. Con la sola unità di base, il telefono fornisce la copertura per una sala di 6,1 x 6,1 m e fino a 10 persone.

Con questo telefono è possibile utilizzare due microfoni di espansione con cavo. Se posizionati lontano dall'unità di base, i microfoni di espansione forniscono una copertura maggiore nelle sale conferenze di dimensioni più grandi. Con l'unità di base e i microfoni di espansione con cavo, il telefono per chiamate in conferenza fornisce la copertura per una sala di 6,1 x 10 m e fino a 22 persone.

Il telefono supporta anche un set opzionale di due microfoni di espansione wireless. Con l'unità di base e i microfoni di espansione wireless, il telefono per chiamate in conferenza fornisce la copertura per una sala di 6,1 x 12,2 m e fino a 26 persone. Per coprire una sala di 6,1 x 12,2 m, si consiglia di posizionare ogni microfono a una distanza massima di 3 m dalla base.

Per aumentare la copertura per una sala, è possibile collegare due unità base. Questa configurazione richiede il kit Collegamento a cascata opzionale e può supportare due microfoni di espansione con cavo o wireless, ma non una combinazione mista. Se si utilizzano microfoni con cavo con il kit Collegamento a cascata, la configurazione fornisce una copertura per una sala fino a 6,1 x 15,2 m e fino a 38 persone. Se si utilizzano microfoni wireless con il kit Collegamento a cascata, la configurazione fornisce una copertura per una sala fino a 6,1 x 17,4 m e fino a 42 persone.

La versione Telefono IP per chiamate in conferenza Cisco 8832NR (non radio) non supporta la rete Wi-Fi, i microfoni di espansione wireless o Bluetooth.

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



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.

Pulsanti e hardware del telefono IP per chiamate in conferenza Cisco 8832





La figura che segue mostra il telefono IP per chiamate in conferenza Cisco 8832.

Figura 2: Pulsanti e funzionalità del telefono IP per chiamate in conferenza Cisco 8832



Nella seguente tabella sono descritti i pulsanti del telefono IP per chiamate in conferenza Cisco 8832.

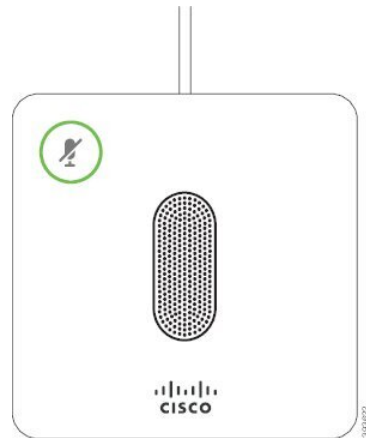
Tabella 5: Telefono IP per chiamate in conferenza Cisco 8832


1	Barra a LED	Indica gli stati della chiamata: <ul style="list-style-type: none"> • Verde fisso: indica una chiamata attiva • Verde lampeggiante: indica una chiamata in arrivo • Verde intermittente: indica una chiamata in attesa • Rosso fisso: indica una chiamata con audio disattivato
2	Porta del microfono di espansione	Il cavo del microfono di espansione è collegato alla porta.
3	Barra disattivazione audio	 Consente di attivare o disattivare il microfono. Quando il microfono è disattivato, la barra del LED è rossa.
4	Pulsanti softkey	 Consente di accedere alle funzioni e ai servizi.
5	Barra di navigazione e pulsante Selezione	 Consente di scorrere i menu, evidenziare le voci e selezionare le voci evidenziate.
6	Pulsante del volume	 Consente di regolare il volume dell'altoparlante (ricevitore sganciato) e il volume della suoneria (ricevitore agganciato). Quando si cambia il volume, la barra a LED si illumina in bianco per mostrare la variazione del volume.

Microfono di espansione con cavo (solo 8832)

Il Cisco IP Conference Phone 8832 supporta due microfoni di espansione con cavo, disponibili nel kit opzionale. Utilizzare i microfoni di espansione nelle sale più grandi o in una sala affollata. Per risultati ottimali, si consiglia di posizionare i microfoni a una distanza tra 0,91 e 2,1 metri dal telefono.

Figura 3: Microfono di espansione con cavo



Durante una chiamata, il LED del microfono di espansione vicino al pulsante **Disattiva audio**  è verde.

Quando il microfono è disattivato, il LED è rosso. Quando si preme il pulsante **Disattiva audio**, viene disattivato l'audio del telefono e dei microfoni di espansione.

Argomenti correlati

[Installazione di microfoni di espansione con cavo](#), a pagina 37

Microfono di espansione wireless (solo 8832)

Il Cisco IP Conference Phone 8832 supporta due microfoni di espansione con cavo, disponibili con base di caricamento in un kit opzionale. Quando il microfono wireless è posizionato sulla base di caricamento, il LED su quest'ultima è illuminato di bianco.

Figura 4: Microfono wireless

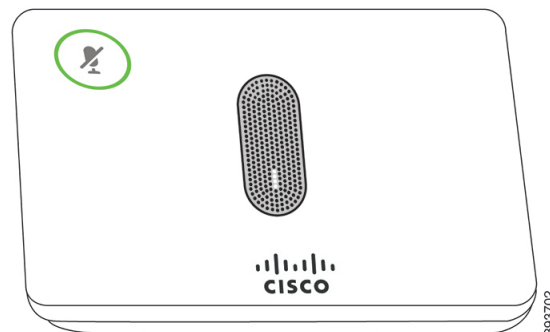
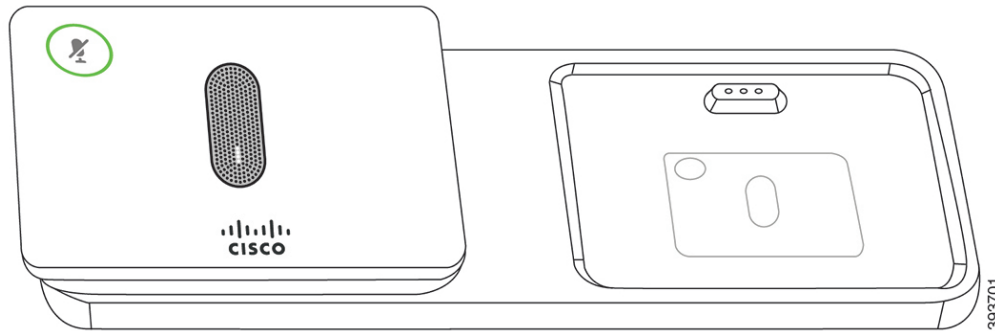



Figura 5: Microfono wireless montato sulla base di caricamento



Quando il telefono per chiamate in conferenza è impegnato in una chiamata, il LED del microfono di espansione vicino al pulsante **Disattiva audio**  è illuminato in verde.

Quando il microfono è disattivato, il LED è illuminato in rosso. Quando si preme il pulsante **Disattiva audio**, viene disattivato l'audio del telefono e dei microfoni di espansione.

Se il telefono è abbinato a un microfono wireless (ad esempio, il microfono wireless 1) e si connette quest'ultimo a un caricabatteria, premendo il softkey **Mostra dettagli** sarà indicato il livello di carica per tale microfono.

Se il telefono è abbinato a un microfono wireless e si connette un microfono con cavo, viene rimosso l'abbinamento del microfono wireless e il telefono viene abbinato al microfono con cavo. Viene visualizzata una notifica sullo schermo del telefono che indica che il microfono con cavo è collegato.

Argomenti correlati

[Installazione dei microfoni di espansione wireless](#), a pagina 38

[Installazione della base di caricamento per microfono wireless](#), a pagina 39

Documentazione correlata

Utilizzare le sezioni indicate di seguito per le relative informazioni.

Documentazione del telefono IP per chiamate in conferenza Cisco 8832

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.

Documentazione di Cisco Unified Communications Manager

Consultare la *Cisco Unified Communications Manager Guida 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 Unified Communications Manager Express

Consultare le pubblicazioni specifiche per la lingua, il modello di telefono e la versione di Cisco Unified Communications Manager Express. Consultare l'URL della documentazione indicato di seguito:

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

Documentazione di Cisco HCS (Hosted Collaboration Service)

Consultare la *Cisco Hosted Collaboration Solution Guida alla documentazione* e altre pubblicazioni specifiche della versione Cisco Hosted Collaboration Solution in uso. Consultare l'URL indicato di seguito:

<https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html>

Documentazione di Cisco Business Edition 4000

Consultare la *Cisco Business Edition 4000 Guida alla documentazione* e altre pubblicazioni specifiche della versione Cisco Business Edition 4000 in uso. Consultare l'URL indicato di seguito:

<https://www.cisco.com/c/en/us/support/unified-communications/business-edition-4000/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/index.php/regulations/export-administration-regulations-ear>.

Differenze terminologiche

In questo documento, il termine *telefono IP Cisco* include il telefono IP per chiamate in conferenza Cisco 8832.

La tabella che segue evidenzia alcune differenze terminologiche nella *Guida per l'utente del telefono IP per chiamate in conferenza Cisco 8832*, nella *Guida all'amministrazione del telefono IP per chiamate in conferenza Cisco 8832 per Cisco Unified Communications Manager* e nella documentazione di Cisco Unified Communications Manager.

Tabella 6: Differenze terminologiche

Guida per l'utente	Guida all'amministrazione
Indicatori messaggio	Indicatore di messaggio in attesa (MWI)
Sistema di posta vocale	Sistema di messaggistica vocale



CAPITOLO 3

Dettagli tecnici

- Specifiche fisiche e dell'ambiente operativo, a pagina 17
- Requisiti di alimentazione dei telefoni, a pagina 18
- Protocolli di rete, a pagina 20
- Interazione con Cisco Unified Communications Manager, a pagina 22
- Interazione con Cisco Unified Communications Manager Express, a pagina 23
- Interazione con il sistema di voice messaging, a pagina 23
- File di configurazione del telefono, a pagina 24
- Comportamento del telefono durante le ore di congestione della rete, a pagina 24
- Application Programming Interface, a pagina 25

Specifiche fisiche e dell'ambiente operativo

La tabella seguente mostra le specifiche fisiche e dell'ambiente operativo per il telefono per chiamate in conferenza.

Tabella 7: 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	Dal 10 al 90% (in assenza di condensa)
Temperatura di conservazione	Da 10 °C a 60 °C (da 14 °F a 140 °F)
Altezza	10,9 mm (278 pollici)
Larghezza	10,9 mm (278 pollici)
Profondità	2,4 mm (61,3 pollici)
Peso	1852 g (4,07 lb)
Alimentazione	IEEE PoE classe 3 tramite un iniettore PoE. Il telefono è compatibile con il Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE). Altre opzioni includono un iniettore Ethernet non PoE se gli switch supportano LLDP-PoE. È necessario un alimentatore del telefono IP per chiamate in conferenza.

Specifica	Valore o intervallo
Funzionalità di sicurezza	Avvio protetto
Cavi	USB-C
Requisiti di distanza	La Specifica Ethernet presume che la lunghezza massima dei cavi tra

Per ulteriori informazioni, vedere la *scheda tecnica del telefono IP per chiamate in conferenza Cisco 8832*:
<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html>

Requisiti di alimentazione dei telefoni

Cisco IP Conference Phone 8832 può utilizzare le seguenti fonti di alimentazione:

- Alimentazione su distribuzione Ethernet (PoE) con Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832
- Distribuzione Ethernet non-PoE con Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832
- Distribuzione Wi-Fi con alimentatore per telefono IP per chiamate in conferenza Cisco 8832

Tabella 8: Linee guida per l'alimentazione del telefono IP per chiamate in conferenza Cisco

Tipo di alimentazione	Linee guida
Alimentazione PoE: fornita da Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832 o Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832 mediante cavo USB-C collegato al telefono.	<p>In caso di utilizzo di Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832 o Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832, per assicurare un funzionamento senza interruzioni del telefono, verificare che lo switch disponga di un'alimentazione di backup.</p> <p>Assicurarsi che la versione CatOS o IOS eseguita sullo switch supporti la distribuzione prevista del telefono. Per informazioni sulla versione del sistema operativo, consultare la documentazione dello switch.</p> <p>Quando si installa un telefono alimentato con PoE, collegare l'iniettore alla LAN prima di collegare il cavo USB-C al telefono. Quando si rimuove un telefono che utilizza PoE, scollegare il cavo USB-C dal telefono prima di rimuovere l'alimentazione dall'adattatore.</p>

Tipo di alimentazione	Linee guida
<p>Alimentatore esterno</p> <ul style="list-style-type: none"> • Distribuzione Ethernet non-PoE con Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832 • Distribuzione Wi-Fi con alimentatore per telefono IP per chiamate in conferenza Cisco 8832 • Distribuzione Ethernet non PoE con Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832 e alimentatore per telefono IP per chiamate in conferenza Cisco 8832 	<p>Quando si installa un telefono alimentato con l'alimentazione esterna, collegare l'iniettore all'alimentatore e all'Ethernet prima di collegare il cavo USB-C al telefono. Quando si rimuove un telefono che utilizza l'alimentazione esterna, scollegare il cavo USB-C dal telefono prima di rimuovere l'alimentazione dall'adattatore.</p>

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.

Argomenti correlati

[Pianificazione della modalità Risparmio energia per il telefono IP Cisco](#), a pagina 113

[Pianificazione di EnergyWise sul telefono IP Cisco](#), a pagina 114

Protocolli di rete

Il telefono Cisco IP Conference Phone 8832 supporta più norme di settore e protocolli di rete Cisco richiesti per la comunicazione voce. Nella tabella seguente viene fornita una panoramica dei protocolli di rete supportati dai telefoni.

Tabella 9: Protocolli di rete supportati dal telefono IP per chiamate in conferenza Cisco

Protocollo di rete	Scopo	Note per l'utilizzo
Bootstrap Protocol (BootP)	BootP consente a un dispositivo di rete, come il telefono, di rilevare determinate informazioni di avvio, ad esempio l'indirizzo IP.	—
CDP (Cisco Discovery Protocol)	CDP è un protocollo di rilevamento dispositivo eseguito su tutte le apparecchiature prodotte da Cisco. Un dispositivo può utilizzare CDP per comunicare la propria presenza ad altri dispositivi e ricevere informazioni sugli altri dispositivi in rete.	Il telefono utilizza CDP per comunicare informazioni di configurazione QoS (Quality of Service) e informazioni di configurazione QoS (Quality of Service).
Dynamic Host Configuration Protocol (DHCP)	DHCP alloca e assegna dinamicamente un indirizzo IP ai dispositivi di rete. 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 presente un gateway e un server TFTP localmente su ogni telefono, il telefono utilizza il server TFTP locale per scaricare il file di configurazione. Si consiglia di utilizzare l'opzione personalizzata DHCP per impostare il valore dell'opzione. Per ulteriori configurazioni DHCP, vedere il capitolo "Configurazione DHCP" di Cisco Unified Communications Manager in uso. Nota Se non è possibile utilizzare l'opzione 1, utilizzare l'opzione 2.
Hypertext Transfer Protocol (HTTP)	HTTP è il protocollo standard per il trasferimento di informazioni e lo spostamento di documenti su Internet e nel Web.	I telefoni utilizzano HTTP per i servizi XML, il protocollo di gestione della configurazione e il protocollo di gestione della configurazione.
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 di Cisco Unified Communications Manager utilizzano l'URL HTTPS. Se la connessione al servizio avviene tramite HTTP, il telefono utilizza il protocollo HTTPS.

Protocollo di rete	Scopo	Note per l'utilizzo
IEEE 802.1x	<p>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.</p> <p>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.</p>	<p>Il telefono implementa lo standard IEEE 802.1X.</p> <p>Se l'autenticazione 802.1X è abilitata sul telefono...</p>
Protocollo Internet (IP)	<p>IP è un protocollo di messaggistica che indirizza e invia pacchetti in rete.</p>	<p>Per comunicare con IP, i dispositivi di rete devono...</p> <p>Le identificazioni di indirizzi IP, subnet e gateway...</p> <p>Configuration Protocol (DHCP). Se non si utilizza il DHCP sul telefono.</p> <p>I telefoni supportano l'indirizzo IPv6. Per ulteriori informazioni, vedere il capitolo "Configurazione di IPv6" del Cisco Unified Communications Manager in uso.</p>
Protocollo LLDP (Link Layer Discovery Protocol)	<p>LLDP è un protocollo di rilevamento di rete standardizzato (simile a CDP) supportato su alcuni dispositivi Cisco e di terze parti.</p>	<p>Il telefono supporta LLDP sulla porta PC.</p>
Protocollo LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	<p>Il protocollo LLDP-MED è un'estensione dello standard LLDP sviluppato per i prodotti voce.</p>	<p>Il telefono supporta LLDP-MED sulla porta SW.</p> <ul style="list-style-type: none"> • Configurazione VLAN vocale • Rilevamento dei dispositivi • Gestione energetica • Gestione delle scorte <p>Per ulteriori informazioni sul supporto del protocollo LLDP-MED, vedere il capitolo "Configurazione di LLDP-MED" del Cisco Unified Communications Manager in uso.</p> <p>Protocol al seguente indirizzo: https://www.cisco.com/en/US/tech/tk652/tk701/...</p>
RTP (Real-Time Transport Protocol)	<p>RTP è un protocollo standard per trasportare dati in tempo reale, come voce e video interattivi, su reti dati.</p>	<p>I telefoni utilizzano il protocollo RTP per inviare dati.</p>
Protocollo RTCP (Real-Time Control Protocol)	<p>RTCP funziona insieme a RTP per fornire dati QoS (come jitter, latenza e ritardo round trip) su flussi RTP.</p>	<p>RTCP è abilitato per impostazione predefinita.</p>
Protocollo Session Description Protocol (SDP)	<p>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.</p>	<p>Le capacità SDP, come ad esempio i tipi di codifiche audio e video, sono determinate su base globale da Cisco Unified Communications Manager. Le capacità SDP supportate da tutti gli endpoint nella conferenza possono consentire la configurazione di tali parametri.</p>

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 consente una rete telefonica a pacchetti. La funzione di segnalazione di rete. La gestione delle sessioni consente di controllare
Protocollo SRTP (Secure Real-Time Transfer protocol)	SRTP è un'estensione del profilo audio/video Real-Time Protocol (RTP) e assicura l'integrità dei pacchetti RTP e Real-Time Control Protocol (RTCP) fornendo autenticazione, integrità e crittografia dei pacchetti dei supporti tra due endpoint.	I telefoni utilizzano SRTP per la crittografia dei supporti
Protocollo TCP (Transmission Control Protocol)	TCP è un protocollo di trasporto orientato alla connessione.	I telefoni utilizzano il protocollo TCP per il collegamento XML.
Protocollo TLS (Transport Layer Security)	TLS è un protocollo standard per la protezione e l'autenticazione delle comunicazioni.	Quando si implementa la sicurezza, i telefoni utilizzano Cisco Unified Communications Manager. Per ulteriori informazioni su Cisco Unified Communications Manager in uso.
Protocollo TFTP (Trivial File Transfer Protocol)	TFTP consente di trasferire i file in rete. Sul telefono, TFTP consente di ottenere un file di configurazione specifico al tipo di telefono.	TFTP richiede un server TFTP nella rete, che può essere diverso da quello sul telefono. Il telefono utilizza un server TFTP diverso da quello sul server TFTP mediante il menu Impostazione rete del telefono. Per ulteriori informazioni, consultare la documentazione di Cisco Unified Communications Manager.
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 di rete

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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 14

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.

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).

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 Administration vengono 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.

Comportamento del telefono durante le ore di congestione della rete

La qualità audio 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.

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.



PARTE **II**

Installazione del telefono IP per chiamate in conferenza Cisco

- [Installazione del telefono, a pagina 29](#)
- [Installazione del telefono su Cisco Unified Communications Manager, a pagina 57](#)
- [Gestione del portale Self Care, a pagina 69](#)



CAPITOLO 4

Installazione del telefono

- Verifica dell'impostazione di rete, a pagina 29
- Onboarding tramite codice di attivazione per telefoni in sede, a pagina 30
- Onboarding tramite codice di attivazione e accesso mobile e remoto, a pagina 31
- Abilitazione della registrazione automatica sul telefono, a pagina 31
- Modalità collegamento a cascata, a pagina 33
- Installazione del telefono per chiamate in conferenza, a pagina 33
- Impostazione del telefono dai menu di configurazione, a pagina 42
- Abilitazione della LAN wireless dal telefono, a pagina 49
- Verifica dell'avvio del telefono, a pagina 55
- Modifica del modello del telefono di un utente, a pagina 56

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 14

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 (Administrative 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**.
-

Modalità collegamento a cascata

È possibile connettere due telefoni per chiamate in conferenza utilizzando un Adattatore smart e i cavi USB-C forniti nel kit Collegamento a cascata per espandere l'area di copertura audio in una sala.

In modalità collegamento a cascata, entrambe le unità ricevono l'alimentazione mediante l'adattatore smart a cui è connesso l'alimentatore. È possibile utilizzare esclusivamente un microfono esterno per unità. È possibile utilizzare una coppia di microfoni con cavo con le unità o una coppia di microfoni wireless con le unità, tuttavia non è una combinazione mista dei microfoni. Quando un microfono con cavo è collegato a una delle unità, ciò rimuove l'abbinamento di eventuali microfoni wireless connessi alla stessa unità. Ogni volta che è presente una chiamata attiva, i LED e le opzioni del menu sullo schermo del telefono di entrambe le unità sono sincronizzati.

Argomenti correlati

- [Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata](#), a pagina 40
- [Un telefono in modalità collegamento a cascata non funziona](#), a pagina 168

Installazione del telefono per chiamate in conferenza

Dopo aver collegato il telefono alla rete, inizia il processo di avvio e il telefono viene registrato in Cisco Unified Communications Manager. Se si disabilita il servizio DHCP, è necessario configurare le impostazioni di rete sul telefono.

Se si utilizza la registrazione automatica, l'utente deve 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.

Dopo aver collegato il telefono, determina se un nuovo caricamento del firmware deve essere installato sul telefono.

Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata, vedere [Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata, a pagina 40](#).

Prima di iniziare

Verificare che la versione del firmware installata su Cisco Unified Communications Manager sia la più recente. Controllare la presenza dei pacchetti aggiornati del dispositivo qui:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Procedura

Passaggio 1

Scegliere la fonte di alimentazione per il telefono:

- Alimentazione su distribuzione Ethernet (PoE) con Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832
- Distribuzione Ethernet non-PoE con Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832
- Distribuzione Wi-Fi con alimentatore per telefono IP per chiamate in conferenza Cisco 8832

Per ulteriori informazioni, consultare [Modalità di alimentazione del telefono per chiamate in conferenza, a pagina 35](#).

Passaggio 2

Collegare il telefono allo switch.

- Se si utilizza PoE:
 1. Collegare il cavo Ethernet alla porta LAN.
 2. Collegare l'altra estremità del cavo Ethernet a Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832 o Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832.
 3. Collegare l'iniettore al telefono per chiamate in conferenza utilizzando il cavo USB-C.
- Se non si utilizza PoE:
 1. Se si utilizza Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832, collegare l'alimentatore alla presa elettrica.
 2. Collegare l'alimentatore all'iniettore Ethernet utilizzando un cavo USB C.
OPPURE
Se si utilizza Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832, collegarlo a una presa elettrica.
 3. Collegare il cavo Ethernet all'iniettore Ethernet non PoE o all'iniettore Ethernet.
 4. Collegare il cavo Ethernet alla porta LAN.
 5. Collegare l'iniettore Ethernet non PoE o l'iniettore Ethernet al telefono per chiamate in conferenza utilizzando un cavo USB-C.
- Se si utilizza il Wi-Fi:

1. Collegare l'alimentatore del telefono IP per chiamate in conferenza Cisco 8832 alla presa elettrica.
2. Collegare l'alimentatore al telefono per chiamate in conferenza utilizzando un cavo USB-C.

Nota Anziché l'alimentatore, è possibile utilizzare l'iniettore Ethernet non PoE per fornire alimentazione al telefono. Tuttavia, è necessario scollegare il cavo LAN. Il telefono si collega alla rete Wi-Fi solo quando la connessione Ethernet non è disponibile.

Passaggio 3	Monitorare il processo di avvio del telefono. Questo passaggio consente di verificare che il telefono sia configurato correttamente.
Passaggio 4	Se non si utilizza la registrazione automatica, configurare manualmente le impostazioni di protezione sul telefono.
Passaggio 5	Consentire al telefono di eseguire l'aggiornamento all'immagine firmware corrente memorizzata su Cisco Unified Communications Manager.
Passaggio 6	Effettuare chiamate con il telefono per verificare che telefono e funzionalità siano correttamente operativi.
Passaggio 7	Fornire informazioni agli utenti 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 Cisco.

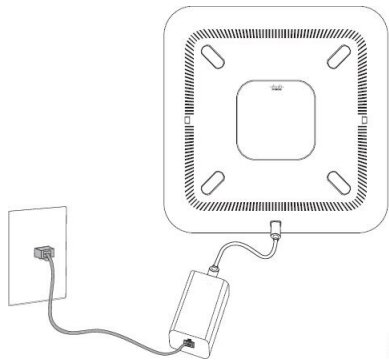
Modalità di alimentazione del telefono per chiamate in conferenza

Il telefono per chiamate in conferenza deve essere alimentato da una di queste fonti:

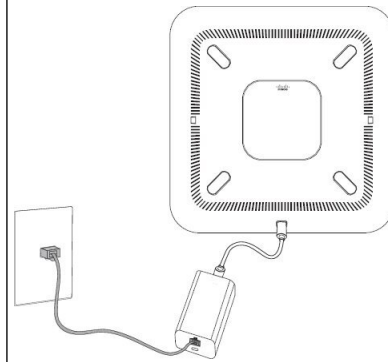
- PoE (Power over Ethernet)
 - Nord America
 - Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832
 - Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832
 - Al di fuori del Nord America: Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832
- Ethernet non PoE
 - Nord America
 - Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832
 - Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832 con un alimentatore del telefono IP per chiamate in conferenza Cisco 8832 collegato a una presa elettrica.
 - Al di fuori del Nord America: Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832
- Wi-Fi: utilizzare l'alimentatore del telefono IP per chiamate in conferenza Cisco 8832 collegato a una presa elettrica.

Figura 6: Opzioni di alimentazione PoE del telefono per chiamate in conferenza

La figura che segue mostra le due opzioni di alimentazione PoE.



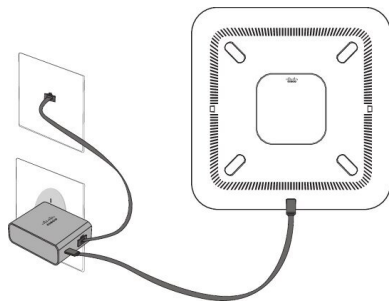
Iniettore PoE per telefono IP per chiamate in conferenza Cisco 8832 con l'opzione di alimentazione PoE



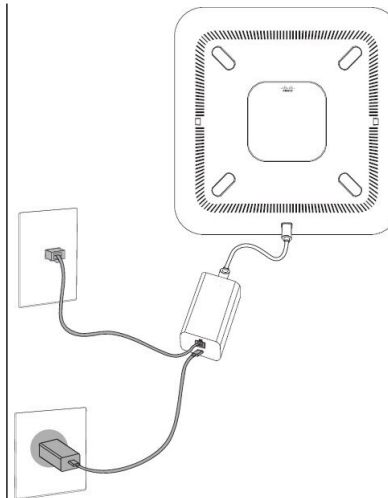
Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832 con l'opzione di alimentazione PoE

Figura 7: Opzioni di alimentazione Ethernet del telefono per chiamate in conferenza

La figura che segue mostra le due opzioni di alimentazione Ethernet.



Iniettore Ethernet non PoE per telefono IP per chiamate in conferenza Cisco 8832 con l'opzione di alimentazione Ethernet



Iniettore Ethernet per telefono IP per chiamate in conferenza Cisco 8832 con l'opzione di alimentazione Ethernet

Figura 8: Opzione di alimentazione del telefono per chiamate in conferenza quando connesso a una rete Wi-Fi

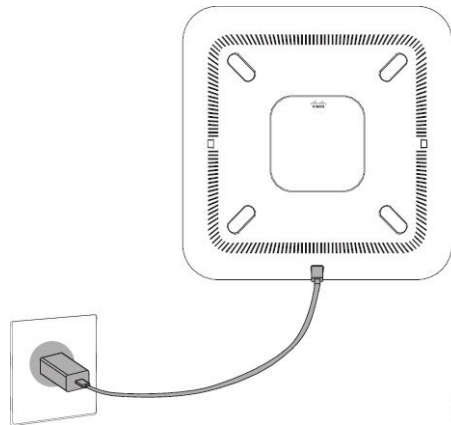
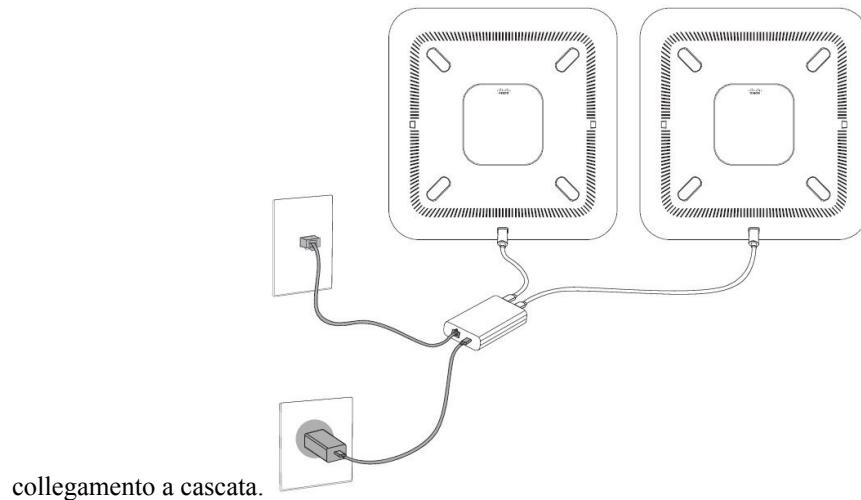


Figura 9: Opzione di alimentazione del telefono per chiamate in conferenza in modalità collegamento a cascata

Nella figura seguente è illustrata l'opzione di alimentazione quando il telefono è collegato in modalità



collegamento a cascata.

Installazione di microfoni di espansione con cavo

Il telefono supporta il kit opzionale con due microfoni di espansione con cavo. È possibile estendere i microfoni fino a una distanza di 2,13 metri dal telefono. Per risultati ottimali, posizionare i microfoni a una distanza tra 0,91 e 2,1 metri dal telefono.

Procedura

Passaggio 1

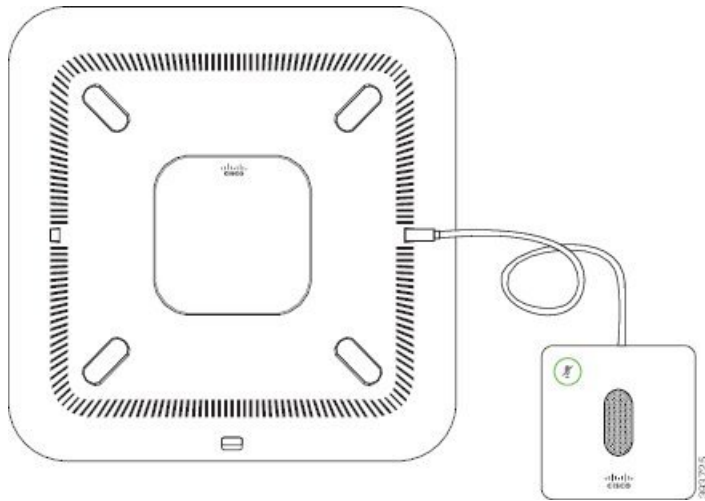
Collegare l'estremità del cavo del microfono alla porta sul lato del telefono.

Passaggio 2

Estendere il cavo del microfono fino a raggiungere la posizione desiderata.

La figura seguente mostra l'installazione di un microfono di espansione con cavo.

Figura 10: Installazione del microfono di espansione con cavo



Installazione dei microfoni di espansione wireless

Il telefono per chiamate in conferenza offre l'opzione di collegamento di due microfoni di espansione wireless.



Nota Con il telefono è necessario utilizzare due microfoni con cavo o due microfoni wireless, ma non una combinazione mista.

Quando il telefono è impegnato in una chiamata, il LED del microfono di espansione è illuminato in verde. Per disattivare l'audio del microfono di espansione, premere il tasto **Disattiva audio**. Quando il microfono è disattivato, il LED è illuminato in rosso. Se la batteria del microfono è quasi esaurita, il LED di indicazione della batteria lampeggia rapidamente.

Prima di iniziare

Prima di installare i microfoni di espansione wireless, scollegare i microfoni di espansione con cavo. Non è possibile utilizzare i microfoni di espansione con cavo e wireless contemporaneamente.

Procedura

Passaggio 1

Posizionare la piastra di montaggio sulla superficie del tavolo dove si desidera collocare il microfono.

Passaggio 2

Rimuovere l'adesivo del nastro biadesivo nella parte inferiore della piastra di montaggio da tavolo. Posizionare la piastra di montaggio da tavolo in modo tale che aderisca alla superficie del tavolo.

Passaggio 3

Collegare il microfono alla piastra di montaggio da tavolo. Nel microfono sono incorporati dei magneti per tenere in posizione l'unità.

Se necessario, è possibile spostare in una posizione diversa sulla superficie del tavolo il microfono e la piastra di montaggio. Prestare attenzione durante lo spostamento per proteggere l'unità.

Argomenti correlati

[Microfono di espansione wireless \(solo 8832\)](#), a pagina 13

[Installazione della base di caricamento per microfono wireless](#), a pagina 39

Installazione della base di caricamento per microfono wireless

Utilizzare la base di caricamento per caricare la batteria del microfono wireless.

Procedura**Passaggio 1**

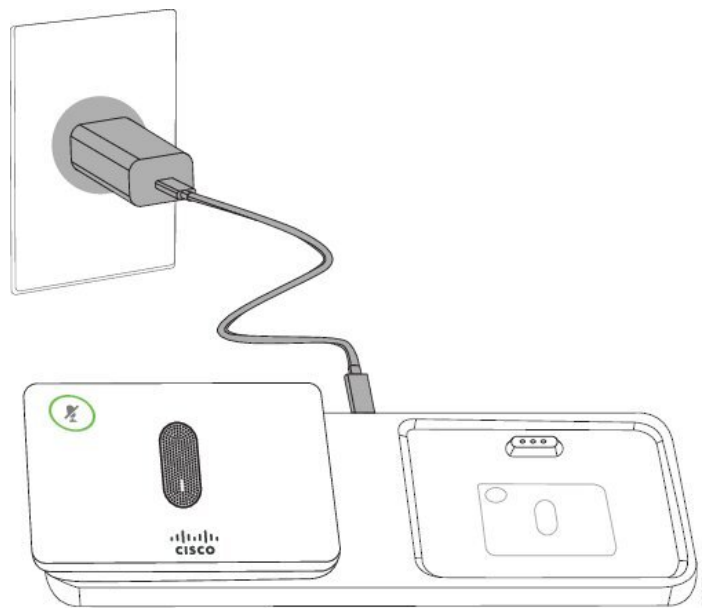
Collegare l'alimentatore della base di caricamento a una presa elettrica.

Passaggio 2

Collegare un'estremità del cavo USB-C nell'apposita base di caricamento e l'altra estremità nell'alimentatore.

La figura seguente mostra l'installazione della base di caricamento per microfono wireless.

Figura 11: Installazione della base di caricamento per microfono wireless



Argomenti correlati

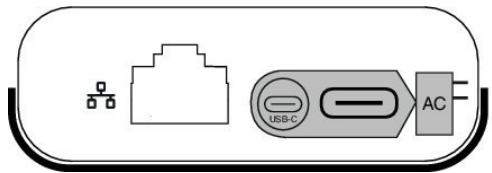
[Microfono di espansione wireless \(solo 8832\)](#), a pagina 13

[Installazione dei microfoni di espansione wireless](#), a pagina 38

Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata

Il kit Collegamento a cascata contiene un Adattatore smart, un cavo LAN corto, due cavi USB-C lunghi e più spessi, nonché un cavo più corto e sottile. In modalità collegamento a cascata, i telefoni per chiamate in conferenza richiedono alimentazione esterna da una presa elettrica. È necessario utilizzare Adattatore smart per collegare i telefoni. I cavi USB-C lunghi devono essere collegati al telefono e il cavo corto all'alimentatore. Fare riferimento alla figura riportata di seguito, quando si connettono alimentatore e porta LAN a Adattatore smart.

Figura 12: Porta dell'adattatore smart e porta LAN



È possibile utilizzare esclusivamente un microfono per unità.



Nota Con il telefono è necessario utilizzare due microfoni con cavo o due microfoni wireless, ma non una combinazione mista.

Il cavo USB-C per l'alimentatore è più sottile rispetto ai cavi USB-C che si collegano al telefono.

Procedura

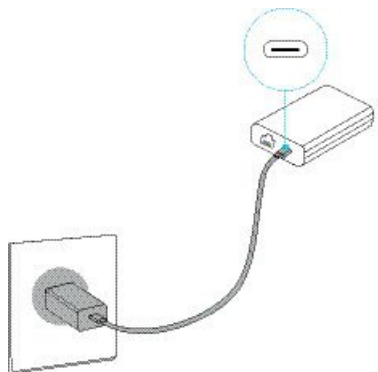
Passaggio 1

Inserire l'alimentatore nella presa elettrica.

Passaggio 2

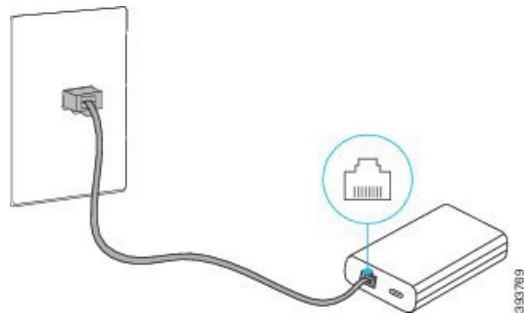
Collegare il cavo USB-C corto e più sottile dall'alimentatore a Adattatore smart.

Figura 13: Porta USB adattatore smart collegata alla presa di alimentazione



Passaggio 3

Required Step Collegare il cavo Ethernet a Adattatore smart e alla porta LAN.

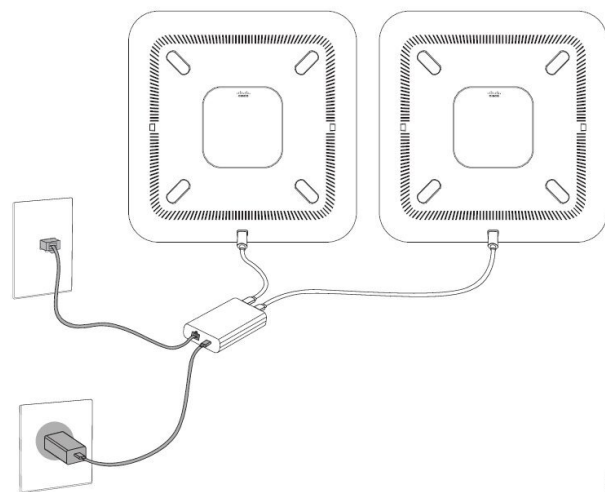
Figura 14: Porta LAN per adattatore smart collegata alla porta LAN sulla presa a muro**Passaggio 4**

Collegare il primo telefono a Adattatore smart utilizzando il cavo USB-C più lungo e più spesso.

Passaggio 5

Collegare il secondo telefono a Adattatore smart utilizzando un cavo USB-C.

La figura seguente mostra l'installazione del telefono per chiamate in conferenza in modalità collegamento a cascata.

Figura 15: Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata**Argomenti correlati**

[Modalità collegamento a cascata](#), a pagina 33

[Un telefono in modalità collegamento a cascata non funziona](#), a pagina 168

Riavvio del telefono per chiamate in conferenza dall'immagine di backup

Il telefono IP per chiamate in conferenza Cisco 8832 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** Tenere premuto il tasto * durante la connessione dell'alimentazione al telefono per chiamate in conferenza.
- Passaggio 2** Dopo che la luce della barra LED si accende di verde e poi si spegne, è possibile rilasciare il tasto *.
- Passaggio 3** Il telefono per chiamate in conferenza si riavvia dall'immagine di backup.
-

Impostazione del telefono dai menu di configurazione

Nel telefono sono incluse diverse impostazioni di rete configurabili che potrebbe essere necessario modificare prima che gli utenti utilizzino il telefono. Tramite i menu del telefono, è possibile accedere a queste impostazioni e modificarne alcune.

Nel telefono sono inclusi i seguenti menu di configurazione:

- Impostazione di rete: fornisce le opzioni per la visualizzazione e la configurazione di diverse impostazioni di rete.
 - Impostazione IPv4: questo sottomenu fornisce ulteriori opzioni di rete.
 - Impostazione IPv6: questo sottomenu fornisce ulteriori opzioni di rete.
- Impostazione protezione: fornisce le opzioni per la visualizzazione e la configurazione di diverse impostazioni di protezione.



Nota È possibile controllare se un telefono dispone dell'accesso al menu Impostazioni o alle opzioni di questo menu. Per controllare l'accesso, utilizzare il campo **Accesso impostazioni** nella Cisco Unified Communications Manager Administration finestra Configurazione telefono. Il campo **Accesso impostazioni** accetta i valori seguenti:


- Enabled: consente l'accesso al menu delle impostazioni.
- Disabilitato: impedisce l'accesso alla maggior parte delle voci nel menu Impostazioni. L'utente può comunque accedere a **Impostazioni > Stato**.
- Limitato: consente l'accesso alle voci di menu di Preferenze utente e Stato e consente di salvare le modifiche al 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 impostazioni**.

In , è possibile configurare le impostazioni di sola visualizzazione sul telefono in Cisco Unified Communications Manager Administration.

Procedura

- Passaggio 1** Premere **Impostazioni**.

- Passaggio 2** Selezionare **Impostazioni amministratore**.
- Passaggio 3** Se richiesto, immettere una password, quindi fare clic su **Registr**.
- Passaggio 4** Selezionare **Impostazione di rete** o **Impostazione protezione**.
- 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 **Indietro** .

Argomenti correlati

- [Riavvio o reimpostazione del telefono per chiamate in conferenza](#), a pagina 175
- [Configurazione delle impostazioni di rete](#), a pagina 44
- [Configurazione delle impostazioni di sicurezza](#).


Applicazione di una password al telefono

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.
-

Voci 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 nel riquadro di navigazione per evidenziare il campo da modificare. Premere **Selez.** 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 il softkey , che consente di eliminare il carattere alla sinistra del cursore.
- Premere **Ripristina** prima di premere **Applica** per ignorare le modifiche apportate.
- Per immettere un punto (ad esempio in un indirizzo IP), premere * sulla tastiera.
- 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.

Configurazione delle impostazioni di rete

Procedura

- Passaggio 1** Premere **Impostazioni**.
- Passaggio 2** Selezionare **Impostazioni amministratore > Impostazione di rete > Impostazione Ethernet**.
- Passaggio 3** Impostare i campi come descritto in [Campi di Impostazione di rete, a pagina 44](#).
Dopo avere impostato i campi, potrebbe essere necessario riavviare il telefono.

Campi di Impostazione di rete

Il menu Impostazione di rete contiene i campi e i menu secondari per IPv4 e IPv6.

Per modificare alcuni campi, è necessario disattivare il protocollo DHCP.

Tabella 10: Menu Impostazione di rete

Voce	Tipo	Impostazione predefinita	Descrizione
Impostazione IPv4	Menu		Vedere la tabella «Sottomenu Impostazione IPv4». Questa opzione viene visualizzata soltanto se il telefono è configurato in modalità Solo IPv4 o in modalità dual-stack.
Impostazione IPv6	Menu		Vedere la tabella «Sottomenu Impostazione IPv6».
Nome host	Stringa		Nome host del telefono. Se si utilizza il protocollo DHCP, il nome viene assegnato automaticamente.
Nome dominio	Stringa		Nome del dominio DNS (Domain Name System) in cui risiede il telefono. Per modificare questo campo, disattivare il protocollo DHCP.

Voce	Tipo	Impostazione predefinita	Descrizione
ID VLAN operativa			VLAN (Virtual Local Area Network) operativa configurata su uno switch Cisco Catalyst a cui appartiene il telefono.
ID VLAN amministrazione			VLAN ausiliaria a cui appartiene il telefono.
Impostazione porta SW	Negoziazione automatica 10 Half 10 Full 100 Half 100 Full	Negoziazione automatica	Velocità e duplex della porta dello switch, dove: <ul style="list-style-type: none"> • 10 Half = 10-BaseT/half duplex • 10 Full = 10-BaseT/full duplex • 100 Half = 100-BaseT/half duplex • 100 Full = 100-BaseT/full duplex
LLDP-MED: porta SW	Disabilitato Abilitato	Abilitato	Indica se il protocollo LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) è abilitato sulla porta dello switch.

Tabella 11: Sottomenu Impostazione IPv4

Voce	Tipo	Impostazione predefinita	Descrizione
DHCP	Disabilitato Abilitato	Abilitato	Consente di abilitare o disabilitare l'utilizzo del protocollo DHCP.
Indirizzo IP			Indirizzo IP (Internet Protocol) versione 4 (IPv4) del telefono. Per modificare questo campo, disattivare il protocollo DHCP.
Subnet mask			Subnet mask utilizzata dal telefono. Per modificare questo campo, disattivare il protocollo DHCP.
Router predefinito 1			Router predefinito utilizzato dal telefono. Per modificare questo campo, disattivare il protocollo DHCP.

Voce	Tipo	Impostazione predefinita	Descrizione
Server DNS 1			Server DNS (Domain Name System) primario (server DNS 1) utilizzato dal telefono. Per modificare questo campo, disattivare il protocollo DHCP.
Server DNS 2			Server DNS (Domain Name System) primario (server DNS 2) utilizzato dal telefono.
Server DNS 3			Server DNS (Domain Name System) primario (server DNS 3) utilizzato dal telefono.
TFTP alternativo	No Si	No	Indica se il telefono utilizza un server TFTP alternativo.
Server TFTP 1			Server TFTP (Trivial File Transfer Protocol) primario utilizzato dal telefono. 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. Consultare le note su TFTP dopo la tabella finale.

Voce	Tipo	Impostazione predefinita	Descrizione
Server TFTP 2			<p>Server TFTP secondario utilizzato dal telefono.</p> <p>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 2. In questo caso, il telefono elimina il 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.</p> <p>Consultare la sezione Note su TFTP dopo la tabella finale.</p>
Indirizzo DHCP rilasciato	No Si	No	

Tabella 12: Sottomenu Impostazione IPv6

Voce	Tipo	Impostazione predefinita	Descrizione
DHCPv6 abilitato	Disabilitato Abilitato	Abilitato	Consente di abilitare o disabilitare l'utilizzo di DHCP IPv6.
Indirizzo IPv6			<p>L'indirizzo IPv6 del telefono.</p> <p>Per modificare questo campo, disattivare il protocollo DHCP.</p>
Lunghezza prefisso IPv6			<p>Lunghezza dell'indirizzo IPv6.</p> <p>Per modificare questo campo, disattivare il protocollo DHCP.</p>
Router predefinito IPv6 1			<p>Router IPv6 predefinito.</p> <p>Per modificare questo campo, disattivare il protocollo DHCP.</p>
Server DNS IPv6 1			<p>Server DNS IPv6 primario</p> <p>Per modificare questo campo, disattivare il protocollo DHCP.</p>
TFTP alternativo IPv6	No Si	No	Indica se il telefono utilizza un server TFTP IPv6 alternativo.

Voce	Tipo	Impostazione predefinita	Descrizione
Server TFTP IPv6 1			Server TFTP IPv6 primario utilizzato dal telefono. Consultare la sezione Note su TFTP dopo la tabella.
Server TFTP IPv6 2			Server TFTP IPv6 secondario utilizzato dal telefono. Consultare la sezione Note su TFTP dopo la tabella.
Indirizzo IPv6 rilasciato	No Sì	No	

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 acquisirà e utilizzerà 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 su IPv6, vedere:

- «Configurazione dispositivo comune» nella *Guida ai servizi e alle funzioni di Cisco Unified Communications Manager*, capitolo «Supporto per gli indirizzi IPv6 su dispositivi Cisco Unified Communications».
- *Guida alla distribuzione di IPv6 per Cisco Collaboration Systems versione 12.0*, disponibile qui: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html>

Note su TFTP

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

Per informazioni sui file CTL e ITL, consultare la *Guida alla protezione di Cisco Unified Communications Manager*.

Impostazione del campo Nome dominio

Procedura

- Passaggio 1** Impostare l'opzione DHCP abilitato su **No**.
- Passaggio 2** Scorrere fino all'opzione Nome dominio, premere **Seleziona**, quindi immettere un nuovo nome di dominio.
- Passaggio 3** Premere **Applica**.
-

Abilitazione della LAN wireless dal telefono

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

Per gli utenti Wi-Fi si consiglia un metodo di roaming veloce e protetto. Si consiglia di utilizzare 802.11 r (FT).

Per informazioni complete sulla configurazione, consultare la *Guida alla distribuzione della LAN wireless per il telefono IP Cisco 8832* alla posizione seguente:

<https://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 8832* 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 **Impostazioni**.
- Passaggio 2** Selezionare **Impostazioni amministratore > Impostazioni di rete > Impostazione client Wi-Fi > Wireless**.
- Passaggio 3** Premere **On**.
-

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 per chiamate in conferenza.



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, deselegionare 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, deselegionare 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 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 per il telefono IP per chiamate in conferenza Cisco 8832* disponibile qui <http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>.

Prima di iniziare

Configurare la LAN wireless da Cisco Unified Communications Manager.

Procedura

- Passaggio 1**
- Passaggio 2**
- Passaggio 3**

Premere **Impostazioni**.

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

Impostare la configurazione wireless come descritto nella tabella seguente.

Tabella 13: Opzioni del menu Impostazione client Wi-Fi

Opzione	Descrizione	Per modificare
Wireless	Accende o spegne la radio wireless sul telefono IP Cisco.	Scorrere fino all'opzione Wireless e premere il switch di attivazione/disattivazione o disattivare l'impostazione.
Nome rete	Consente di connettersi a una rete wireless mediante la finestra Scegli una rete . Questa finestra contiene due softkey: Indietro e Altro .	Nella finestra Scegli una rete , selezionare la rete a cui si desidera collegarsi.
Accesso registrazione Wi-Fi	Abilita la visualizzazione della finestra registrazione Wi-Fi.	Scorrere fino all'opzione Accesso Wi-Fi e utilizzare lo switch di attivazione/disattivazione per attivare l'impostazione.
Impostazione IPv4	Nel menu secondario di configurazione Impostazione IPv4, è possibile effettuare le operazioni seguenti: <ul style="list-style-type: none"> • 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 la tabella "Sottomenu Impostazione IPv4".	Scorrere fino all'opzione Impostazione IPv4 e premere Seleziona .

Opzione	Descrizione	Per modificare
Impostazione IPv6	<p>Nel menu secondario di configurazione Impostazione IPv6, è possibile effettuare le operazioni seguenti:</p> <ul style="list-style-type: none"> • 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. <p>Per ulteriori informazioni sui campi dell'indirizzo IPv6, consultare la tabella "Sottomenu Impostazione IPv6".</p>	Scorrere fino all'opzione Impostazione IPv6 e premere Seleziona .
Indirizzo MAC	Indirizzo MAC (Media Access Control) univoco del telefono.	Solo visualizzazione. Impossibile modificare.
Nome dominio	Nome del dominio DNS (Domain Name System) in cui risiede il telefono.	Consultare Impostazione del campo Nome dominio , a pagina 49.

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 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-MSCHAPv2 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 telefoni non supportano il metodo TFTP per l'installazione del certificato.

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.

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**.

Verifica dell'avvio del telefono

Una volta collegato il telefono a una fonte di alimentazione, viene avviato automaticamente il processo diagnostico di avvio.

Procedura

Accendere il telefono.

Se viene visualizzata la schermata principale, è stato avviato correttamente.

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.

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

Installazione del telefono su Cisco Unified Communications Manager

- [Impostazione di un telefono IP per chiamate in conferenza Cisco](#), a pagina 57
- [Individuazione dell'indirizzo MAC del telefono](#), a pagina 62
- [Metodi di aggiunta del telefono](#), a pagina 62
- [Aggiunta degli utenti a Cisco Unified Communications Manager](#), a pagina 63
- [Aggiunta di un utente a un gruppo di utenti finali](#), a pagina 65
- [Associazione dei telefoni agli utenti](#), a pagina 66
- [SRST \(Survivable Remote Site Telephony\)](#), a pagina 66

Impostazione di un telefono IP per chiamate in conferenza Cisco

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

Per ulteriori informazioni su uno di questi passaggi, 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: vedere [Individuazione dell'indirizzo MAC del telefono](#), a pagina 62
- Ubicazione fisica del telefono
- Nome o ID utente dell'utente del telefono
- Gruppo dispositivi

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

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

Passaggio 2

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

Per ulteriori informazioni, consultare la documentazione sulle licenze specifica della versione di Cisco Unified Communications Manager in uso.

Passaggio 3

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

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

Passaggio 4

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 5

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 6

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

Passaggio 7

Configurare il telefono. Selezionare **Dispositivo > Telefono**.

- Individuare il telefono da modificare o aggiungere un nuovo telefono.
- Configurare il telefono compilando i campi richiesti nel riquadro Informazioni dispositivo della finestra Configurazione telefono.
 - Indirizzo MAC (richiesto): accertare che il valore comprenda 12 caratteri esadecimale
 - Descrizione: immettere una descrizione utile nel caso sia necessario cercare informazioni su questo utente
 - Gruppo dispositivi (richiesto)
 - Profilo telefono comune
 - Area ricerca chiamate
 - Posizione
 - Proprietario (Utente o Anonimo) e, se è selezionato Utente, l'ID utente proprietario

Il dispositivo con le impostazioni predefinite viene aggiunto al database Cisco Unified Communications Manager.

Per informazioni sui campi di configurazione specifici del prodotto, consultare «?» Guida pulsanti nella finestra Configurazione telefono e il collegamento correlato.

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.

- c) Nell'area Informazioni specifiche sul prodotto di questa finestra, scegliere un Profilo di protezione dispositivo e impostare la modalità di protezione.

Nota Scegliere un profilo di protezione basato sulla strategia di sicurezza globale dell'azienda. Se il telefono non supporta la protezione, scegliere un profilo non sicuro.

- d) Nell'area Informazioni interno, selezionare la casella di controllo Abilita mobilità interni se il telefono supporta la mobilità interni Cisco.
e) Fare clic su **Salva**.

Passaggio 8

Per impostare i parametri SIP, selezionare **Dispositivo > Impostazioni dispositivo > Profilo SIP**.

Passaggio 9

Selezionare **Dispositivo > Telefono** per configurare i numero di rubrica (linee) sul telefono compilando i campi richiesti nella finestra Configurazione numero di rubrica.

- a) Individuare il telefono.
b) Nella finestra Configurazione telefono, fare clic su Linea 1 nel riquadro di sinistra.

I telefoni per chiamate in conferenza hanno solo una linea.

- c) Nel campo Numero di rubrica, immettere un numero valido da chiamare.

Nota Il campo deve contenere lo stesso numero che appare nel campo Numero di telefono della finestra Configurazione utente finale.

- d) Dall'elenco a discesa Partizione indirizzamento, scegliere la partizione a cui appartiene il numero di rubrica. Se si desidera limitare l'accesso al numero di rubrica, scegliere <None> per la partizione.
e) Dall'elenco a discesa Area ricerca chiamate, scegliere l'area ricerca chiamate appropriata. Il valore scelto si applica a tutti i dispositivi che utilizzano questo numero di rubrica.
f) Nell'area Inoltro chiamata e Impostazioni Risposta per Assente, scegliere le voci (ad esempio, InoltroTutte, Inoltro se occupato interno) e le destinazioni corrispondenti a cui inviare le chiamate.

Esempio:

Se si desidera deviare le chiamate interne ed esterne che ricevono il segnale di occupato alla casella vocale per questa linea, selezionare la casella di controllo Casella vocale accanto alle voci Devia se occupato e Devia se occupato esterna nella colonna di sinistra dell'area Risposta per Assente e Impostazioni inoltro chiamata.

- g) Nel riquadro Linea 1 su dispositivo, configurare i campi seguenti:

- Display (campo ID chiamante interno): è possibile immettere nome e cognome dell'utente di questo dispositivo in modo che il nome venga visualizzato per tutte le chiamate interne. Lasciare vuoto questo campo per visualizzare l'interno del telefono.
- Maschera numero di telefono esterno: indicare il numero di telefono (o maschera) utilizzato per inviare le informazioni sull'ID chiamante quando si effettua una chiamata da questa linea. È possibile

immettere fino a 24 caratteri numerici e «X». Le X rappresentano il numero di rubrica e devono comparire alla fine dello schema.

Esempio:

Se si specifica una maschera di 408902XXXX, una chiamata esterna dall'interno 6640 visualizza un numero di ID chiamante 4089026640.

Questa impostazione si applica solo al dispositivo corrente, a meno che non si selezioni la casella di controllo a destra (Aggiorna impostazioni dispositivo condiviso) e si faccia clic su **Propaga impostazioni selezionate**. La casella di controllo a destra viene visualizzata solo se altri dispositivi condividono questo numero di rubrica.

h) Selezionare **Salva**.

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

Passaggio 10

(Facoltativo) Associare l'utente a un telefono. Fare clic su **Associa utenti finali** al fondo della finestra Configurazione telefono per associare un utente finale alla linea configurata.

- a) Utilizzare **Trova** insieme con i campi Cerca per individuare l'utente.
- b) Selezionare la casella accanto al nome utente e fare clic su **Aggiungi selezionato**.

Il nome utente e l'ID utente compaiono nel riquadro Utenti associati a linea della finestra Configurazione numero di rubrica.

c) Selezionare **Salva**.

L'utente è ora associato alla Linea 1 sul telefono.

Passaggio 11

(Facoltativo) Associare l'utente al dispositivo.

- a) Scegliere **Gestione utente > Utente finale**.
- b) Utilizzare le caselle di ricerca e **Trova** per individuare l'utente aggiunto.
- c) Fare clic sull'ID utente.
- d) Nell'area Associazioni numero di rubrica della schermata, impostare l'Interno primario dall'elenco a discesa.
- e) (Facoltativo) Nell'area Informazioni mobilità, selezionare la casella Abilita mobilità.
- f) Nell'area Informazioni autorizzazioni, utilizzare i pulsanti **Aggiungi a gruppo di controllo degli accessi** 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.

- g) Per visualizzare i dettagli del gruppo, selezionarlo e fare clic su **Vedi dettagli**.
- h) Nell'area Mobilità interni, selezionare la casella Abilita Extension Mobility Cross Cluster se l'utente può utilizzare tale servizio.
- i) Nell'area Informazioni dispositivo, fare clic su **Associazioni dispositivo**.
- j) Utilizzare i campi di ricerca e **Trova** per individuare il dispositivo da associare all'utente.
- k) Selezionare il dispositivo e fare clic su **Salva selezionati/modifiche**.
- l) Fare clic su **Vai** accanto al collegamento correlato «Torna all'utente» nell'angolo superiore destro della schermata.
- m) Selezionare **Salva**.

Passaggio 12

Personalizzare i modelli di softkey. Selezionare **Dispositivo > Impostazioni dispositivo > Modello softkey**.

Utilizzare la pagina per aggiungere, eliminare o modificare l'ordine delle funzioni dei softkey visualizzati sul telefono dell'utente in base alle esigenze di utilizzo.

Il telefono per chiamate in conferenza ha requisiti speciali per i softkey. Per ulteriori informazioni, vedere i collegamenti correlati.

Passaggio 13

Configurare i servizi del telefono IP Cisco e assegnare i servizi. Selezionare **Dispositivo > Impostazioni dispositivo > Servizi telefono**.

Fornisce servizi IP al telefono.

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

Passaggio 14

(Facoltativo) Aggiungere le informazioni utente alla rubrica globale per Cisco Unified Communications Manager. Selezionare **Gestione utente > Utente finale**, quindi fare clic su **Aggiungi nuovo** e configurare i campi obbligatori. I campi obbligatori sono contrassegnati da un asterisco (*).

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 per utilizzare la rubrica LDAP esistente, consultare [Impostazione della rubrica aziendale, a pagina 127](#). Dopo aver abilitato il campo **Abilita sincronizzazione dal server LDAP**, non sarà possibile aggiungere altri utenti da Cisco Unified Communications Manager Administration.

- a) Impostare i campi ID utente e Cognome.
- b) Assegnare una password (per il portale Self Care).
- c) Assegnare un PIN (per Mobilità interni Cisco ed Elenco personale).
- d) Associare l'utente a un telefono.

Gli utenti controllano le funzioni del telefono, ad esempio l'inoltro delle chiamate o l'aggiunta di numeri di chiamata rapida o servizi.

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

Passaggio 15

(Facoltativo) Associare un utente a un gruppo di utenti. Selezionare **Gestione utente > Impostazioni utente > Gruppo di controllo degli accessi**.

Assegna gli utenti a un elenco comune di ruoli e autorizzazioni validi per tutti gli utenti in 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.

Affinché gli utenti finali possano accedere al portale Self Care di Cisco Unified Communications, occorre aggiungerli al gruppo di utenti finali standard Cisco Communications Manager.

Argomenti correlati

[Configurazione specifica del prodotto](#), a pagina 99

[Funzioni e impostazione del telefono IP per chiamate in conferenza Cisco](#), a pagina 95

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

[Impostazione di un nuovo modello di softkey](#), a pagina 96

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, selezionare **Impostazioni** > **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 62.

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

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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 14

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 14

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 64.

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 14

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 le comunicazioni con il Cisco Unified Communications Manager di controllo sono interrotte. 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 informazioni su SRST, vedere: <https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/tsd-products-support-series-home.html>

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

Tabella 14: Supporto funzione SRST

Funzione	Supportata	Note
Nuova chiamata	Si	
Termina	Si	
Ripeti	Si	
Rispondi	Si	
Attesa	Si	
Riprendi	Si	
Conferenza	Si	Solo 3 vie e mixing locale.
Elenco partecipanti conferenza	No	
Trasferisci	Si	Solo consultazione.
Trasferimento a chiamate attive (Trasferimento diretto)	No	
Risposta automatica	Si	
Avviso di chiamata	Si	
ID chiamante	Si	
Presentazione sessione unificata	Si	Conferenza è la sola funzione supportata a causa di altre limitazioni delle funzioni.
Casella vocale	Si	La casella vocale non verrà sincronizzata con altri utenti nel cluster Cisco Unified Communications Manager.
Inoltro di tutte le chiamate	Si	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	Si	
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.
Indicazione avanzata messaggio in attesa	Sì	Sullo schermo del telefono vengono visualizzati i simboli del numero di messaggi.
Parcheggio chiamate indirizzate	No	La softkey non viene visualizzata.
Ripristino attesa	Sì	
Attesa remota	No	Le chiamate vengono visualizzate come chiamate in attesa locali.
Conferenza automatica	No	La softkey ConfAut non viene visualizzata.
RispAss	Sì	
Risposta per assente di gruppo	No	La softkey non viene visualizzata.
Risposta per altri gruppi	No	La softkey non viene visualizzata.
ID chiamata indesiderata	Sì	
QRT	Sì	
Gruppo di ricerca	No	La softkey non viene visualizzata.
Mobilità	No	La softkey non viene visualizzata.
Privacy	No	La softkey non viene visualizzata.
Prenotazione di chiamata	No	La softkey Prenota non viene visualizzata.
URL del servizio	Sì	Non viene visualizzato il tasto di linea programmabile con un URL di servizio assegnato.



CAPITOLO 6

Gestione del portale Self Care

- [Panoramica del portale Self Care, a pagina 69](#)
- [Impostazione dell'accesso degli utenti al portale Self Care, a pagina 69](#)
- [Personalizzazione della visualizzazione del portale Self Care, a pagina 70](#)

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 14

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 per chiamate in conferenza Cisco

- [Sicurezza del telefono IP per chiamate in conferenza Cisco, a pagina 73](#)
- [Personalizzazione del telefono IP per chiamate in conferenza Cisco, a pagina 91](#)
- [Funzioni e impostazione del telefono IP per chiamate in conferenza Cisco, a pagina 95](#)
- [Rubrica aziendale ed Elenco personale, a pagina 127](#)



CAPITOLO 7

Sicurezza del telefono IP per chiamate in conferenza Cisco

- [Panoramica sulla protezione del telefono IP Cisco, a pagina 73](#)
- [Miglioramento della protezione della rete telefonica, a pagina 74](#)
- [Funzioni di protezione supportate, a pagina 75](#)

Panoramica sulla protezione del telefono IP Cisco

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.

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

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

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

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.

Il telefono IP per chiamate in conferenza Cisco 8832 è conforme agli Standard FIPS (Federal Information Processing Standard). Per il corretto funzionamento della modalità FIPS, è necessario impostare una dimensione di chiave RSA di 2048 bit o superiore. Se la dimensione del certificato del server RSA 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. Il messaggio "La dimensione della chiave del certificato non è conforme a FIPS" è visualizzato nei messaggi di stato del telefono.

Non è possibile utilizzare le chiavi private (LSC o MIC) in modalità FIPS.

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

Argomenti correlati

[Impostazione di un LSC \(Locally Significant Certificate\)](#), a pagina 77

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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 per Proxy 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>).

- *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>)
- *SIP OAuth: Guida alla configurazione delle funzionalità di Cisco Unified Communications Manager* (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-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.

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.

La tabella che segue fornisce una panoramica delle funzioni di protezione supportate dal telefono IP per chiamate in conferenza Cisco 8832. Per ulteriori informazioni su queste funzioni, sulla protezione di Cisco Unified Communications Manager e del telefono IP Cisco, vedere la documentazione della particolare versione di Cisco Unified Communications Manager.

Tabella 15: Panoramica delle funzioni di protezione

Funzione	Descrizione
Autenticazione immagine	I file binari con firma (con estensione .sbn) impediscono la manomissione. La manomissione con l'immagine impedisce al telefono di eseguire l'operazione.
Installazione certificato del sito del cliente	Ogni telefono richiede un certificato univoco per l'autenticazione (Certificate), ma per ulteriore sicurezza, è possibile specificare un certificato tramite CAPF (Certificate Authority Proxy Function) dal menu di configurazione della protezione del telefono.
Autenticazione dispositivo	Si verifica tra il server Cisco Unified Communications Manager e il telefono se deve essere stabilita una connessione protetta tra il telefono e il server. Il percorso di segnalazione protetto tra le due entità mediante il protocollo SRTP, a meno che non possano essere autenticati da Cisco Unified Communications Manager.
Autenticazione file	Convalida i file con firma digitale scaricati dal telefono. Il telefono convalida i file dopo la creazione. I file che non vengono autenticati non vengono utilizzati per l'ulteriore elaborazione.
Autenticazione segnalazione	Utilizza il protocollo TLS per convalidare l'assenza di manomissioni.
MIC (Manufacturing Installed Certificate)	Ciascun telefono contiene un certificato MIC (Manufacturing Installed Certificate). MIC è una garanzia univoca permanente di identità per il telefono.
Riferimento SRST sicuro	Dopo aver configurato un riferimento SRST per sicurezza e qualità, Cisco Unified Communications Manager Administration, il server TFTP aggiunge il certificato SRST. Il telefono utilizza quindi una connessione TLS per interagire con il route.
Crittografia supporti	Utilizza SRTP per garantire che i flussi dei supporti tra dispositivi siano protetti. Comprende la creazione di una coppia di chiavi primaria e secondaria e della consegna delle chiavi durante il loro trasporto.

Funzione	Descrizione
CAPF (Certificate Authority Proxy Function)	Implementa parti della procedura di generazione del certificato con il telefono per la generazione di chiavi e l'installazione di autorità di certificazione specificate dal cliente per conto di
Profili di sicurezza	Definisce se il telefono è in stato non protetto, autenticato o
File di configurazione crittografati	Consente di garantire la privacy dei file di configurazione o
Disabilitazione opzionale della funzionalità del server Web per un telefono	È possibile impedire l'accesso a una pagina Web del telefono
Aumento della sicurezza del telefono	Ulteriori opzioni di protezione, controllabili da Cisco Unified <ul style="list-style-type: none"> Disabilitare l'accesso alle pagine Web di un telefono <p>Nota È possibile visualizzare le impostazioni correnti di configurazione del telefono.</p>
Autenticazione 802.1X	Il telefono può utilizzare l'autenticazione 802.1X per richieste
Crittografia AES 256	Quando sono collegati a Cisco Unified Communications Manager, i telefoni supportano AES 256 per TLS e SIP per la segnalazione e la crittografia (SIP 1.2 tramite codici basati su AES-256 conformi a standard Secure Processing Standards). Questi nuovi codici sono: <ul style="list-style-type: none"> Per connessioni TLS: <ul style="list-style-type: none"> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Per sRTP: <ul style="list-style-type: none"> AEAD_AES_256_GCM AEAD_AES_128_GCM <p>Per ulteriori informazioni, consultare la documentazione di</p>
Certificati Elliptic Curve Digital Signature Algorithm (ECDSA)	Come parte della certificazione dei criteri comuni (CC), Cisco Unified Communications Manager versione 11.0. Ciò ha effetto su tutti i prodotti VOS (Voice Office System) successive.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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, scegliere **Impostazioni**.

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.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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 per le connessioni tra due telefoni. È possibile configurare, tramite un ponte conferenza protetto, le funzioni Conferenza protetta, Mobilità interni telefonici di Cisco e Linee condivise.


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 16: 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 crittografata

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 automatica	Il livello minimo di protezione è crittografato.	L'utente che ha avviato la conferenza riceve Non rispetta il livello di protezione chiamata rifiutata.
Protetto	Conferenza automatica	Il livello minimo di protezione non è protetto.	Ponte conferenza protetto Nella conferenza vengono accettate tutte le

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. È supportato soltanto il metodo PEAP-MSCHAPv2. Il metodo PEAP-GTC non è supportato.

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 17: Schemi di autenticazione e crittografia

Configurazione telefono IP Cisco	Configurazione AP			
	Sicurezza	Gestione delle chiavi	Crittografia	Roaming veloce
Nessuno	Nessuno	Nessuno	Nessuno	N/D
WEP	WEP statica	Statica	WEP	N/D

Configurazione telefono IP Cisco	Configurazione AP			
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

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>

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.

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: <ul style="list-style-type: none"> 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. |
| Passaggio 2 | Aprire un browser Web e immettere il seguente URL, dove <i>indirizzo_IP</i> è l'indirizzo IP del telefono IP Cisco:
<code>https://<IP_address>:8443</code> |
| 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** Selezionare il certificato sul PC.
- Passaggio 3** Nel campo **Password di estrazione**, immettere la password di estrazione del certificato.
- Passaggio 4** Fare clic su **Carica**.
- Passaggio 5** 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 supporto dell'autenticazione 802.1X richiede diversi componenti:

- Telefono IP Cisco: il telefono avvia la richiesta di accesso alla rete. I telefoni 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.
- 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.

- 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.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14



CAPITOLO 8

Personalizzazione del telefono IP per chiamate in conferenza Cisco

- [Suonerie personalizzate del telefono, a pagina 91](#)
- [Personalizzazione del segnale di linea, a pagina 93](#)

Suonerie personalizzate del telefono

Il telefono IP Cisco viene fornito con due tipi di suonerie predefinite implementate nell'hardware: Chirp1 e Chirp2. 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 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.



Attenzione Per tutti i nomi di file viene applicata la distinzione tra lettere maiuscole e minuscole. Se per il nome file non si utilizzano correttamente le maiuscole e le minuscole, le modifiche non vengono applicate sul telefono.

Per ulteriori informazioni, consultare il capitolo "Squilli e sfondi personalizzati" della [Guida alla configurazione delle funzionalità per Cisco Unified Communications Manager](#).

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

Impostazione di una suoneria personalizzata

Procedura

- Passaggio 1** Creare un file PCM per ciascuna suoneria personalizzata (una suoneria per file). Assicurarsi che i file PCM siano conformi alle guide linea del formato elencate nella sezione Formati di file delle suonerie personalizzate.
- Passaggio 2** Caricare i nuovi file PCM creati sul server TFTP di Cisco per ciascuna unità Cisco Unified Communications Manager presente nel cluster.

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

Passaggio 3

Salvare le modifiche e chiudere il file Ringlist-wb.

Passaggio 4

Per memorizzare nella cache il nuovo file Ringlist-wb:

- Arrestare e avviare il servizio TFTP tramite Cisco Unified Serviceability
- Disabilitare e abilitare nuovamente il parametro del servizio TFTP «Abilita memorizzazione nella cache dei file costanti e bin all'avvio», posizionato nell'area Parametri di servizio avanzati.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

Formati di file delle suonerie personalizzate

Il file Ringlist-wb.xml definisce un oggetto XML contenente un elenco dei tipi di suonerie del telefono. Questo file include fino a 50 tipi di suonerie. Ciascun tipo di suoneria contiene un puntatore al file PCM utilizzato per il tipo di suoneria specifico e il testo visualizzato nel menu Tipo suoneria sul telefono IP Cisco per quel tipo di suoneria specifico. Questo file è presente nel server TFTP di ogni Cisco Unified Communications Manager.

L'oggetto XML CiscoIPPhoneRinglist utilizza il seguente set di etichette semplici per la descrizione delle informazioni:

```
<CiscoIPPhoneRingList>
  <Ring>
    <DisplayName/>
    <FileName/>
  </Ring>
</CiscoIPPhoneRingList>
```

Le caratteristiche seguenti si applicano ai nomi definizione. È necessario includere il DisplayName e il FileName richiesti per ciascun tipo di suoneria del telefono.

- DisplayName consente di specificare il nome della suoneria personalizzata per il file PCM associato che verrà visualizzato nel menu Tipo suoneria del telefono IP Cisco.
- FileName consente di specificare il nome del file PCM per la suoneria personalizzata da associare a DisplayName.



Nota I valori immessi nei campi DisplayName e FileName non possono superare i 25 caratteri.

Questo esempio mostra un file Ringlist-wb.xml in cui vengono definiti due tipi di suoneria del telefono:

```
<CiscoIPPhoneRingList>
  <Ring>
    <DisplayName>Analog Synth 1</DisplayName>
    <FileName>Analog1.rwb</FileName>
  </Ring>
  <Ring>
    <DisplayName>Analog Synth 2</DisplayName>
    <FileName>Analog2.rwb</FileName>
  </Ring>
</CiscoIPPhoneRingList>
```

I file PCM delle suonerie devono rispettare i seguenti requisiti per poter essere riprodotti correttamente sui telefoni IP Cisco:

- PCM non elaborato (nessuna intestazione)
- 8.000 campioni al secondo
- 8 bit a campione
- Compressione mu-law
- Dimensione massima suoneria = 16080 campioni
- Dimensione minima suoneria = 240 campioni
- Numero di campioni nella suoneria = multipli di 240
- La suoneria inizia e finisce al passaggio per lo zero.

Per creare dei file PCM per le suonerie personalizzate del telefono, utilizzare un qualsiasi pacchetto standard di modifica audio in grado di supportare questi requisiti del formato di file.

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: <ul style="list-style-type: none">• Esterno• Interno• Impostazione predefinita |
| Passaggio 6 | Selezionare Salva . |
| Passaggio 7 | Riavviare i telefoni. |
-



CAPITOLO 9

Funzioni e impostazione del telefono IP per chiamate in conferenza Cisco

- [Supporto utente per il telefono IP Cisco, a pagina 95](#)
- [Migrazione diretta del telefono a un telefono multiplatforma, a pagina 95](#)
- [Impostazione di un nuovo modello di softkey, a pagina 96](#)
- [Configurazione dei servizi telefonici per gli utenti, a pagina 97](#)
- [Configurazione delle funzioni del telefono, a pagina 97](#)

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

Migrazione diretta del telefono a un telefono multiplatforma

È possibile eseguire facilmente la migrazione del proprio aziendale telefono a un telefono multiplatforma 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

Impostazione di un nuovo modello di softkey

Per consentire agli utenti di accedere ad alcune funzioni, è necessario aggiungere i softkey a un modello di softkey. Ad esempio, per consentire agli utenti di utilizzare la funzione Non disturbare, è necessario abilitare il softkey. Per ulteriori informazioni, consultare la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.

Si consiglia di creare diversi modelli. Ad esempio, creare un modello per il telefono in una sala conferenze e un altro modello per un telefono nell'ufficio di un dirigente.

Questa procedura illustra i passaggi per creare un nuovo modello di softkey e assegnarlo a un telefono specifico. Analogamente a altre funzioni del telefono, è possibile utilizzare anche il modello per tutti i telefoni per chiamate in conferenza o un gruppo di telefoni.

Procedura

-
- Passaggio 1** Accedere a Cisco Unified Communications Manager Administration come amministratore.
- Passaggio 2** Selezionare **Dispositivo > Impostazioni dispositivo > Modello softkey**.
- Passaggio 3** Fare clic su **Trova**.
- Passaggio 4** Selezionare una delle seguenti opzioni:
- Cisco Unified Communications Manager 11.5 e le versioni precedenti: **Utente standard**
 - Cisco Unified Communications Manager 12.0 e versioni successive: **Personal Conference User** (Utente conferenza personale) o **Public Conference User** (Utente conferenza pubblica).
- Passaggio 5** Fare clic su **Copia**.
- Passaggio 6** Modificare il nome del modello.
- Ad esempio, Modello sala conferenze 8832.
- Passaggio 7** Fare clic su **Salva**.
- Passaggio 8** Accedere alla pagina **Configura layout softkey** dal menu in alto a destra.
- Passaggio 9** Per ogni stato della chiamata, impostare le funzioni da visualizzare.
- Passaggio 10** Fare clic su **Salva**.
- Passaggio 11** Torna alla pagina **Trova/Elenca** dal menu in alto a destra.
- Il nuovo modello viene visualizzato nell'elenco dei modelli.
- Passaggio 12** Selezionare **Dispositivo > Telefono**.
- Passaggio 13** Individuare il telefono per il nuovo modello e selezionarlo.
- Passaggio 14** Nel campo **Modello softkey**, selezionare il nuovo modello di softkey.
- Passaggio 15** Fare clic su **Salva e Applica configurazione**.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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. Il telefono IP gestisce ogni servizio come applicazione separata.

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 [Panoramica del portale Self Care, a pagina 69](#) per un riepilogo delle informazioni che occorre fornire agli utenti finali.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

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.

Argomenti correlati

[Configurazione di credenziali utente persistenti per l'accesso a Expressway](#), a pagina 123

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. |

Argomenti correlati

[Configurazione specifica del prodotto](#), a pagina 99

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.

Argomenti correlati

[Configurazione specifica del prodotto](#), a pagina 99

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.

Argomenti correlati

[Configurazione specifica del prodotto](#), a pagina 99

Configurazione specifica del prodotto

Nella tabella seguente vengono descritti i campi del riquadro Layout configurazione specifica del prodotto. Alcuni campi in questa tabella vengono visualizzate solo nella pagina **Dispositivo > Telefono**.

Tabella 18: Campi di Configurazione specifica del prodotto

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Accesso alle impostazioni	Disabilitato Abilitato Limitato	Abilitato	Abilita, disabilita o limita l'accesso alle impostazioni di configurazione locali nell'applicazione Impostazioni. Con accesso limitato, è possibile accedere ai menu Preferenze e Informazioni di sistema. Sono inoltre accessibili alcune impostazioni nel menu Wi-Fi. Con accesso disabilitato, nel menu Impostazioni non sono visualizzate opzioni.
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.
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	Abilitato	Controlla l'utilizzo di TLS 1.2 per una connessione al server Web. <ul style="list-style-type: none"> • 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
Composizione Enbloc	Disabilitato Abilitato	Disabilitato	<p>Controlla il metodo di composizione.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Giorni retroilluminazione non attiva	Giorni della settimana		<p>Definisce i giorni in cui la retroilluminazione non si accende automaticamente all'ora specificata nel campo Ora accensione retroilluminazione.</p> <p>Scegliere i giorni dall'elenco a discesa. Per scegliere più di un giorno, selezionare tutti i giorni desiderati tenendo premuto il tasto Ctrl.</p> <p>Consultare Pianificazione della modalità Risparmio energia per il telefono IP Cisco, a pagina 113.</p>
Ora accensione retroilluminazione	hh:mm		<p>Definisce l'ora in cui la retroilluminazione si accende automaticamente ogni giorno (tranne nei giorni specificati nel campo Giorni retroilluminazione non attiva).</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>Ad esempio, per accendere automaticamente la retroilluminazione alle 07:00 (0700), immettere 07:00. Per accendere la retroilluminazione alle 14:00 (1400), immettere 14:00.</p> <p>Se questo campo è vuoto, la retroilluminazione si accende automaticamente alle 00:00.</p> <p>Consultare Pianificazione della modalità Risparmio energia per il telefono IP Cisco, a pagina 113.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Durata accensione retroilluminazione	hh:mm		<p>Definisce l'intervallo di tempo in cui la retroilluminazione resta accesa dopo essersi acceso all'ora specificata nel campo Ora accensione retroilluminazione.</p> <p>Ad esempio, per mantenere la retroilluminazione accesa per 4 ore e 30 minuti in seguito all'accensione automatica, immettere 04:30.</p> <p>Se questo campo è vuoto, il telefono si spegne automaticamente alla fine della giornata (00:00).</p> <p>Se il campo Ora accensione retroilluminazione è impostato su 0:00 e il campo della durata della retroilluminazione è vuoto (o è impostato su 24:00), la retroilluminazione non si spegne.</p> <p>Consultare Pianificazione della modalità Risparmio energia per il telefono IP Cisco, a pagina 113.</p>
Timeout retroilluminazione non attiva	hh:mm		<p>Definisce l'intervallo di tempo in cui il telefono non è attivo prima dello spegnimento della retroilluminazione. Si applica solo se la retroilluminazione è stata accesa da un utente (tramite la pressione di un pulsante sul telefono o il sollevamento del ricevitore) mentre era spenta in base alla pianificazione impostata.</p> <p>Ad esempio, per spegnere la retroilluminazione dopo 1 ora e 30 minuti di inattività del telefono in seguito all'accensione della retroilluminazione da parte dell'utente, immettere 01:30.</p> <p>Consultare Pianificazione della modalità Risparmio energia per il telefono IP Cisco, a pagina 113.</p>
Accensione retroilluminazione con chiamata in arrivo	Disabilitato Abilitato	Abilitato	Accende la retroilluminazione quando è in arrivo una chiamata.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Abilita Power Save Plus	Giorni della settimana		<p>Definisce la pianificazione dei giorni in cui il telefono si spegne.</p> <p>Scegliere i giorni dall'elenco a discesa. Per scegliere più di un giorno, selezionare tutti i giorni desiderati tenendo premuto il tasto Ctrl.</p> <p>Se Abilita Power Save Plus è attivato, si riceverà un messaggio di avviso sui problemi di ricezione delle chiamate di emergenza (e911).</p> <p>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.</p> <p>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.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Ora accensione telefono	hh:mm		<p>Determina l'ora di accensione automatica del telefono nei giorni indicati nel campo Abilita Power Save Plus.</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>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.</p> <p>Il valore predefinito è vuoto e corrisponde alle 00:00.</p> <p>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.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>
Ora spegnimento telefono	hh:mm		<p>Definisce 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.</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>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.</p> <p>Il valore predefinito è vuoto e corrisponde alle 00:00.</p> <p>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.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Timeout inattività spegnimento telefono	hh:mm		<p>Indica l'intervallo di tempo in cui il telefono resta inattivo prima di spegnersi.</p> <p>Il timeout si verifica nelle seguenti condizioni:</p> <ul style="list-style-type: none"> • 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 riaccessso dallo switch collegato. • Quando viene raggiunta l'ora di spegnimento del telefono ma il telefono è in uso. <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>
Abilita avviso acustico	Casella di controllo	Non selezionata	<p>Quando abilitato, invia al telefono l'istruzione di riprodurre un avviso acustico 10 minuti prima dell'ora specificata nel campo Ora spegnimento telefono.</p> <p>Questa casella di controllo viene applicata soltanto se nella casella Abilita Power Save Plus sono selezionati uno o più giorni.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>
Dominio EnergyWise	Fino a 127 caratteri		<p>Identifica il dominio EnergyWise in cui si trova il telefono.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>
Segreto EnergyWise	Fino a 127 caratteri		<p>Identifica la password segreta di protezione utilizzata per comunicare con gli endpoint nel dominio EnergyWise.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Consenti sostituzioni EnergyWise	Casella di controllo	Non selezionata	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>Per disabilitare Power Save Plus, è necessario deselegionare 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.</p> <p>Consultare Pianificazione di EnergyWise sul telefono IP Cisco, a pagina 114.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
<p> Criterio Collega e Trasferimento diretto </p>	<p> Abilitazione Stessa linea Disabilitazione Stessa linea </p>	<p> Abilitazione Stessa linea, Più linee </p>	<p> Controlla la possibilità di collegare e trasferire le chiamate. </p> <ul style="list-style-type: none"> • Abilitazione Stessa linea, Più linee: gli utenti possono trasferire o collegare direttamente la chiamata corrente a un'altra chiamata sulla stessa linea. • Disabilitazione Stessa linea: 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.
<p> Tono durante registrazione </p>	<p> Disabilitato Abilitato </p>	<p> Disabilitato </p>	<p> Controlla la riproduzione del tono quando un utente registra una chiamata. </p>
<p> Volume locale tono registrazione </p>	<p> Numero intero da 0 a 100 </p>	<p> 100 </p>	<p> Controlla il volume del tono di registrazione per l'utente locale. </p>
<p> Volume remoto tono registrazione </p>	<p> Numero intero da 0 a 100 </p>	<p> 50 </p>	<p> Controlla il volume del tono di registrazione per l'utente remoto. </p>
<p> Durata tono registrazione </p>	<p> Numero intero da 1 a 3000 millisecondi </p>		<p> Controlla la durata del tono di registrazione. </p>
<p> Server di registro </p>	<p> Stringa di 256 caratteri al massimo </p>		<p> Identifica il server syslog IPv4 per l'output di debug del telefono. </p> <p> Il formato per l'indirizzo è: indirizzo: <port>@@base=<0-7>;pfs=<0-1> </p>
<p> Registro remoto </p>	<p> Disabilitato Abilitato </p>	<p> Disabilitato </p>	<p> Controlla la possibilità di inviare i registri al server syslog. </p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Profilo registro	Impostazione predefinita Preimpostato Telefonia SIP UI Rete Supporti Aggiornamento Accessorio Protezione EnergyWise MobileRemoteAccess	Preimpostato	Specifica il profilo di registrazione predefinito. <ul style="list-style-type: none"> • 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 • Energywise: vengono registrate informazioni sul risparmio energetico • MobileRemoteAccess: vengono registrate informazioni sull'accesso mobile e remoto tramite Expressway
Server di registro IPv6	Stringa di 256 caratteri al massimo		Identifica il server syslog IPv6 per l'output di debug del telefono.
Cisco Discovery Protocol (CDP): porta dello switch	Disabilitato Abilitato	Abilitato	Controlla Cisco Discovery Protocol sul telefono.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): porta dello switch	Disabilitato Abilitato	Abilitato	Abilita LLDP-MED sulla porta SW.
ID dell'Asset LLDP	Stringa di 32 caratteri al massimo		Identifica l'ID dell'asset assegnato al telefono per la gestione delle scorte.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Energy Efficient Ethernet (EEE): porta dello switch	Disabilitato Abilitato	Disabilitato	Controlla l'EEE sulla porta dello switch.
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 Disabilitato Abilitato	Controllato dall'utente	Specifica lo stato della funzione di autenticazione 802.1x. <ul style="list-style-type: none"> • 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.
Configurazione remota porta switch	Disabilitato Negoziazione automatica 10 Half 10 Full 100 Half 100 Full	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.
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).
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.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Registra registro chiamate da linea condivisa	Disabilitato Abilitato	Disabilitato	Specifica se registrare il registro chiamate da una linea condivisa.
Volume suoneria minimo	0 - Silenzioso 1–15	0 - Silenzioso	Controlla il volume minimo della suoneria del telefono.
Peer Firmware Sharing	Disabilitato Abilitato	Abilitato	<p>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.</p> <p>Condivisione del firmware:</p> <ul style="list-style-type: none"> • 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.
Server di caricamento	Stringa di 256 caratteri al massimo		Identifica il server IPv4 alternativo utilizzato dal telefono per scaricare il firmware e gli aggiornamenti.
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.

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
Rileva errore di connessione a Unified CM	Normale Ritardato	Normale	<p>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.</p> <p>I valori validi specificano Normale (il rilevamento di un errore di connessione di Unified CM si verifica alla velocità di sistema standard) o Ritardato (il rilevamento di un errore di connessione a Unified CM si verifica circa quattro volte più lentamente rispetto all'impostazione Normale).</p> <p>Scegliere Normale per riconoscere più rapidamente un errore di connessione di Unified CM. Selezionare Ritardato se si preferisce che il failover venga leggermente ritardato per consentire di ristabilire la connessione.</p> <p>L'esatta differenza temporale tra il rilevamento dell'errore di connessione Normale e Ritardato dipende da numerose variabili che cambiano continuamente.</p>
ID requisito speciale	Stringa		Controlla le funzioni personalizzate dei caricamenti ES (Engineering Special).
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.
Credenziali utente persistenti per l'accesso a Expressway	Disabilitato Abilitato	Disabilitato	<p>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).</p> <p>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.</p> <p>Per ulteriori informazioni, vedere la sezione Configurazione di credenziali utente persistenti per l'accesso a Expressway, a pagina 123.</p>

Nome campo	Tipo di campo o scelte	Impostazione predefinita	Descrizione
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 Configurazione di credenziali utente persistenti per l'accesso a Expressway , a pagina 123.
Disabilita crittografie TLS	Consultare Disabilitazione delle crittografie TLS (Transport Layer Security) , a pagina 112.	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.
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.

Argomenti correlati

[Configurazione di credenziali utente persistenti per l'accesso a Expressway](#), a pagina 123

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>).

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.

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 19: 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.

Campo	Descrizione
Ora accensione display	<p>L'ora in cui il display si accende automaticamente ogni giorno (tranne nei giorni specificati nel campo Giorni display non attivo).</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>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.</p> <p>Se questo campo è vuoto, il display si accenderà automaticamente alle 00:00.</p>
Durata accensione display	<p>Intervallo di tempo in cui il display resta acceso dopo essersi acceso all'ora specificata nel campo Ora accensione display.</p> <p>Immettere in questo campo un valore nel formato <i>ore:minuti</i>.</p> <p>Ad esempio, per mantenere il display acceso per 4 ore e 30 minuti in seguito all'accensione automatica, immettere 04:30.</p> <p>Se questo campo è vuoto, il telefono si spegnerà automaticamente alla fine della giornata (00:00).</p> <p>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.</p>
Timeout display non attivo	<p>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.</p> <p>Immettere in questo campo un valore nel formato <i>ore:minuti</i>.</p> <p>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.</p> <p>Il valore predefinito è 01:00.</p>

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.

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 20: Campi di configurazione EnergyWise

Campo	Descrizione
Abilita Power Save Plus	<p>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.</p> <p>Per impostazione predefinita, non è selezionato nessun giorno.</p> <p>Se il campo Abilita Power Save Plus è selezionato, si riceverà un messaggio di avviso sui problemi di ricezione delle chiamate di emergenza (e911).</p> <p>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.</p> <p>Nota Per disabilitare Power Save Plus, è necessario deselegionare 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.</p>

Campo	Descrizione
Ora accensione telefono	<p>Determina l'ora di accensione automatica del telefono nei giorni indicati nel campo Abilita Power Save Plus.</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>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.</p> <p>Il valore predefinito è vuoto e corrisponde alle 00:00.</p> <p>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.</p>
Ora spegnimento telefono	<p>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.</p> <p>Immettere in questo campo un orario nel formato di 24 ore, dove con 00:00 si indica mezzanotte.</p> <p>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.</p> <p>Il valore predefinito è vuoto e corrisponde alle 00:00.</p> <p>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.</p>
Timeout inattività spegnimento telefono	<p>Intervallo di tempo in cui il telefono resta inattivo prima di spegnersi.</p> <p>Il timeout si verifica nelle seguenti condizioni:</p> <ul style="list-style-type: none"> • 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 riaccessso dallo switch collegato. • Quando viene raggiunta l'ora di spegnimento del telefono ma il telefono è in uso. <p>L'intervallo dei valori di questo campo va da 20 a 1440 minuti.</p> <p>Il valore predefinito è 60 minuti.</p>

Campo	Descrizione
Abilita avviso acustico	<p>Quando abilitato, invia al telefono l'istruzione di riprodurre un avviso acustico 10 minuti prima dell'ora specificata nel campo Ora spegnimento telefono.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>Questa casella di controllo viene applicata soltanto se nella casella Abilita Power Save Plus sono selezionati uno o più giorni.</p>
Dominio EnergyWise	<p>Dominio EnergyWise in cui si trova il telefono.</p> <p>La lunghezza massima di questo campo è di 127 caratteri.</p>
Segreto EnergyWise	<p>Password segreta di protezione utilizzata per comunicare con gli endpoint nel dominio EnergyWise.</p> <p>La lunghezza massima di questo campo è di 127 caratteri.</p>
Consenti sostituzioni EnergyWise	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

- Passaggio 4** Selezionare **Salva**.
- Passaggio 5** Selezionare **Applica configurazione**.
- Passaggio 6** Riavviare il telefono.

Impostazione dell'opzione Non disturbare

Quando è attiva la funzione Non disturbare (NoDist), l'intestazione sulla schermo telefono per chiamate in conferenza diventa di colore rosso.

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.
 - 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 14

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**.

Impostazione del parametro UCR 2008

I parametri che supportano UCR 2008 si trovano in Cisco Unified Communications Manager Administration. Nella tabella seguente vengono descritti tali parametri e viene indicato il percorso per la modifica delle impostazioni.

Tabella 21: Posizione del parametro UCR 2008

Parametro	Percorso di amministrazione
Modalità FIPS	Dispositivo > Impostazioni dispositivo > Profilo telefono comune
	Sistema > Configurazione telefono aziendale
	Dispositivo > Telefoni
Accesso SSH	Dispositivo > Telefono
	Dispositivo > Impostazioni dispositivo > Profilo telefono comune

Parametro	Percorso di amministrazione
Accesso Web	Dispositivo > Telefono
	Sistema > Configurazione telefono aziendale
	Dispositivo > Impostazioni dispositivo > Profilo telefono comune
Sistema > Configurazione telefono aziendale	
Modalità indirizzi IP	Dispositivo > Impostazioni dispositivo > Configurazione dispositivo comune
Preferenza Modalità indirizzi IP per Segnalazione	Dispositivo > Impostazioni dispositivo > Configurazione dispositivo comune

Impostazione del parametro UCR 2008 in Configurazione dispositivo comune

Seguire questa procedura per impostare i parametri UCR 2008 seguenti:

- Modalità indirizzi IP
- Preferenza Modalità indirizzi IP per Segnalazione

Procedura

-
- Passaggio 1** In Cisco Unified Communications Manager Administration, selezionare **Dispositivo > Impostazioni dispositivo > Configurazione dispositivo comune**.
- Passaggio 2** Impostare il parametro Modalità indirizzi IP.
- Passaggio 3** Impostare la Preferenza Modalità indirizzi IP per il parametro Segnalazione.
- Passaggio 4** Selezionare **Salva**.
-

Impostazione del parametro UCR 2008 in Profilo telefono comune

Seguire questa procedura per impostare i parametri UCR 2008 seguenti:

- Modalità FIPS
- Accesso SSH
- Accesso Web

Procedura

-
- Passaggio 1** In Cisco Unified Communications Manager Administration, selezionare **Dispositivo > Impostazioni dispositivo > Profilo telefono comune**.

- Passaggio 2** Impostare il parametro Modalità FIPS su **Abilitato**.
- Passaggio 3** Impostare il parametro Accesso SSH su **Disabilitato**.
- Passaggio 4** Impostare il parametro Accesso Web su **Disabilitato**.
- Passaggio 5** Impostare il parametro SRTCP a 80 bit su **Abilitato**.
- Passaggio 6** Selezionare **Salva**.
-

Impostazione del parametro UCR 2008 in Configurazione telefono aziendale

Seguire questa procedura per impostare i parametri UCR 2008 seguenti:

- Modalità FIPS
- Accesso Web

Procedura

- Passaggio 1** In Cisco Unified Communications Manager Administration, selezionare **Sistema > Configurazione telefono aziendale**.
- Passaggio 2** Impostare il parametro Modalità FIPS su **Abilitato**.
- Passaggio 3** Impostare il parametro Accesso Web su **Disabilitato**.
- Passaggio 4** Selezionare **Salva**.
-

Impostazione del parametro UCR 2008 in Telefono

Seguire questa procedura per impostare i parametri UCR 2008 seguenti:

- Modalità FIPS
- Accesso SSH
- Accesso Web

Procedura

- Passaggio 1** In Cisco Unified Communications Manager Administration, selezionare **Dispositivo > Telefono**.
- Passaggio 2** Impostare il parametro Accesso SSH su **Disabilitato**.
- Passaggio 3** Impostare il parametro Modalità FIPS su **Abilitato**.
- Passaggio 4** Impostare il parametro Accesso Web su **Disabilitato**.
- Passaggio 5** Selezionare **Salva**.
-

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).

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

La tabella seguente mostra diversi scenari di distribuzione per Mobile and Remote Access Through Expressway.

Scenario	Azioni
L'utente in sede accede alla rete aziendale, dopo aver implementato Mobile and Remote Access Through Expressway.	La rete aziendale viene rilevata e il telefono si registra normalmente in Cisco Unified Communications Manager.
L'utente fuori sede accede alla rete aziendale con Mobile and Remote Access Through Expressway.	<p>Il telefono rileva che si trova in modalità fuori sede, viene visualizzata la finestra di connessione di Mobile and Remote Access Through Expressway e l'utente si collega alla rete aziendale.</p> <p>Gli utenti devono avere un nome di servizio valido, nome utente e password per collegarsi alla rete.</p> <p>Prima di poter accedere alla rete aziendale, gli utenti devono 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.</p> <p>Se si implementa un telefono nuovo, gli utenti possono ignorare il requisito di ripristino delle impostazioni di rete.</p> <p>Gli utenti, se hanno un'opzione DHCP 150 o 66 abilitata sul loro router di rete, potrebbero non riuscire ad accedere alla rete aziendale. Gli utenti devono disabilitare tali impostazioni DHCP o configurare direttamente il loro indirizzo IP statico.</p>

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 97

[Configurazione specifica del prodotto](#), a pagina 99

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**.
-



CAPITOLO 10

Rubrica aziendale ed Elenco personale

- [Impostazione della rubrica aziendale, a pagina 127](#)
- [Impostazione dell'Elenco personale, a pagina 127](#)

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.

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 14

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

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.

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.



PARTE **IV**

Risoluzione dei problemi del telefono IP per chiamate in conferenza Cisco

- [Monitoraggio dei sistemi telefonici, a pagina 131](#)
- [Risoluzione dei problemi del telefono, a pagina 157](#)
- [Manutenzione, a pagina 175](#)
- [Supporto utente internazionale, a pagina 179](#)



CAPITOLO 11

Monitoraggio dei sistemi telefonici

- [Panoramica sul monitoraggio dei sistemi telefonici](#), a pagina 131
- [Stato del telefono IP Cisco](#), a pagina 131
- [Pagina Web del telefono IP Cisco](#), a pagina 142
- [Richiesta di informazioni dal telefono in formato XML](#), a pagina 153

Panoramica sul monitoraggio dei sistemi telefonici

È possibile visualizzare diverse informazioni sul telefono mediante il relativo menu di stato e le pagine Web. Tali informazioni comprendono:

- Informazioni dispositivo
- Informazioni di configurazione di rete
- Statistiche di rete
- Log dei dispositivi
- Statistiche di flusso

Questo capitolo descrive le informazioni che è possibile ottenere dalla 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.

Argomenti correlati

[Risoluzione dei problemi del telefono](#), a pagina 157

Stato del telefono IP Cisco

Le sezioni seguenti descrivono come visualizzare le informazioni sul modello, i messaggi di stato e le statistiche di rete sul telefono IP Cisco.

- 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.

Visualizzazione della finestra Informazioni telefono

Procedura

-
- Passaggio 1** Premere **Impostazioni > Informazioni di sistema**.
- Passaggio 2** Per uscire dal menu, premere **Esci**.
-

Visualizzazione del menu Stato

Procedura

-
- Passaggio 1** Premere **Impostazioni > Stato**.
- Passaggio 2** Per uscire dal menu, premere **Esci**.
-

Visualizzazione della finestra Messaggi di stato

Procedura

-
- Passaggio 1** Premere **Impostazioni > Stato > Messaggi di stato**.
- Passaggio 2** Per uscire dal menu, premere **Esci**.
-

Campi di Messaggi di stato

Nella tabella seguente vengono descritti i messaggi di stato visualizzati nella schermata Messaggi di stato del telefono.

Tabella 22: Messaggi di stato sul telefono IP Cisco

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 server DHCP e l'indirizzo IP per il telefono.

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 telefono.
Errore checksum ROM	Il file del software scaricato è danneggiato.	Ottenere una nuova copia del firmware nella directory TFTPPath. Occorre cancellare la directory solo quando il software è scaricato. In caso contrario, i file possono danneggiarsi.
IP duplicato	Un altro dispositivo utilizza l'indirizzo IP assegnato al telefono.	Se il telefono ha un indirizzo IP statico, assicurarsi che non sia assegnato un indirizzo IP duplicato. Se si utilizza DHCP, controllare la configurazione DHCP.
Cancellazione dei file CTL e ITL	Cancellazione del file CTL o ITL.	Nessuna. Questo messaggio è solo informativo.
Errore aggiorn. impost. internaz.	Impossibile trovare uno o più file di localizzazione nella directory del percorso TFTP, oppure i file non sono validi. Le impostazioni internazionali non sono state modificate.	Da Cisco Unified Operating System, assicurarsi che i file seguenti si trovino nelle directory di gestione dei file TFTP: <ul style="list-style-type: none"> • Ubicato nella directory secondaria delle impostazioni internazionali di default: <ul style="list-style-type: none"> • tones.xml • Ubicati nella directory secondaria delle impostazioni internazionali di default: <ul style="list-style-type: none"> • 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 telefono viene aggiunto al database di Cisco Unified Communications Manager. Se il telefono non viene registrato, Cisco Unified Communications Manager genera una risposta File Configuration Not Found . <ul style="list-style-type: none"> • Il telefono non è registrato in Cisco Unified Communications Manager. Occorre aggiungere il telefono al database di Cisco Unified Communications Manager e abilitare la registrazione automatica. • Se si utilizza il DHCP, verificare che il server TFTP sia configurato correttamente. • Se si utilizzano gli indirizzi IP statici, verificare che la configurazione del server TFTP sia corretta.

Messaggio	Descrizione	Spiegazione possibile e azione
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 ancora utilizzare il cluster Cisco Unified Communications Manager.
Indirizzo IP rilasciato	Il telefono è configurato per rilasciare l'indirizzo IP.	Il telefono rimane in stand-by finché non riceve un nuovo indirizzo IP o si reimposta l'indirizzo DHCP.
Timeout DHCP IPv4	Il server DHCP IPv4 non risponde.	<p>La rete è occupata: gli errori si risolvono con la riduzione del carico di rete.</p> <p>Nessuna connettività di rete tra il server e il telefono: verificare le connessioni di rete.</p> <p>Il server DHCP IPv4 è inattivo: controllare lo stato del server DHCP IPv4.</p> <p>Gli errori persistono: provare ad assegnare un indirizzo IP statico.</p>
Timeout DHCP IPv6	Il server DHCP IPv6 non risponde.	<p>La rete è occupata: gli errori si risolvono con la riduzione del carico di rete.</p> <p>Nessuna connettività di rete tra il server e il telefono: verificare le connessioni di rete.</p> <p>Il server DHCP IPv6 è inattivo: controllare lo stato del server DHCP IPv6.</p> <p>Gli errori persistono: provare ad assegnare un indirizzo IP statico.</p>
Timeout DNS IPv4	Il server DNS IPv4 non risponde.	<p>La rete è occupata: gli errori si risolvono con la riduzione del carico di rete.</p> <p>Nessuna connettività di rete tra il server e il telefono: verificare le connessioni di rete.</p> <p>Il server DNS IPv4 è inattivo: controllare lo stato del server DNS IPv4.</p>
Timeout DNS IPv6	Il server DNS IPv6 non risponde.	<p>La rete è occupata: gli errori si risolvono con la riduzione del carico di rete.</p> <p>Nessuna connettività di rete tra il server e il telefono: verificare le connessioni di rete.</p> <p>Il server DNS IPv6 è inattivo: controllare lo stato del server DNS IPv6.</p>
Host DNS IPv4 sconosciuto	Il DNS IPv4 non è in grado di risolvere il nome del server TFTP o di Cisco Unified Communications Manager.	<p>Verificare che i nomi host del server TFTP e del Cisco Unified Communications Manager siano configurati correttamente nel file hosts del telefono e nel server DNS IPv4.</p> <p>Provare a utilizzare gli indirizzi IPv4 in formato numerico.</p>

Messaggio	Descrizione	Spiegazione possibile e azione
Host DNS IPv6 sconosciuto	Il DNS IPv6 non è in grado di risolvere il nome del server TFTP o di Cisco Unified Communications Manager.	Verificare che i nomi host del server TFTP o di Cisco Unified Communications Manager siano corretti. Provare a utilizzare gli indirizzi IPv6.
Caric. HC non riuscito	L'applicazione scaricata non è compatibile con l'hardware del telefono.	Si verifica se si è tentato di installare un'applicazione sul telefono che non supporta le modalità di caricamento. Controllare l'ID del carico assegnato dal server TFTP o di Cisco Unified Communications Manager, scegliere un ID compatibile. Reinserire il carico visualizzato sul telefono.
Nessun router predefinito	DHCP o la configurazione statica non ha specificato alcun router predefinito.	Se il telefono dispone di un indirizzo IP statico, il router predefinito sia configurato. Se si utilizza il DHCP, il server DHCP deve avere un router predefinito. Controllare la configurazione.
Nessun server DNS IPv4	È stato specificato un nome ma DHCP o la configurazione IP statica non ha specificato alcun indirizzo del server DNS IPv4.	Se il telefono ha un indirizzo IP statico, il server DNS IPv4 sia configurato. Se si utilizza DHCP, il server DHCP deve avere un server DNS IPv4. Controllare la configurazione.
Nessun server DNS IPv6	È stato specificato un nome ma DHCP o la configurazione IP statica non ha specificato alcun indirizzo del server DNS IPv6.	Se il telefono ha un indirizzo IP statico, il server DNS IPv6 sia configurato. Se si utilizza DHCP, il server DHCP deve avere un server DNS IPv6. Controllare la configurazione.
Nessuna Trust List installata	Il file CTL o il file ITL non è installato nel telefono.	La Trust List non è configurata su Cisco Unified Communications Manager, che non ha un'impostazione predefinita. La Trust List non è configurata. Per ulteriori informazioni sulle Trust Lists, vedere la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
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 sono state apportate al telefono in Cisco Unified Communications Manager ed è stato premuto Applica configurazione . Applicare le modifiche.
Errore accesso TFTP	Il server TFTP punta a una directory inesistente.	Se si utilizza il DHCP, verificare che il server TFTP sia configurato correttamente. Se si utilizzano indirizzi IP statici, verificare che il server TFTP sia configurato correttamente.

Messaggio	Descrizione	Spiegazione possibile e azione
Errore TFTP	Il telefono non riconosce un codice di errore fornito dal server TFTP.	Contattare Cisco TAC (Technical Assistance Center).
Timeout TFTP	Il server TFTP non risponde.	La rete è occupata: gli errori si risolvono con la riduzione del carico di rete. Nessuna connettività di rete tra il server e il telefono: verificare le connessioni di rete. Il server TFTP è inattivo: controllare lo stato del 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 dell'autenticazione se non è configurato sullo switch.
Aggiornamento della Trust List non riuscito	Aggiornamento non riuscito dei file CTL e ITL.	Nel telefono sono installati i file CTL e ITL. È possibile effettuare l'aggiornamento ai file CTL e ITL. Possibili motivi dell'errore: <ul style="list-style-type: none"> • Si è verificato un guasto di rete. • Il server TFTP non era attivo. • Il nuovo token di sicurezza utilizzato per il telefono e il certificato TFTP utilizzato per il server sono stati introdotti, ma non sono disponibili i file CTL e ITL correnti installati nel telefono. • Si è verificato un errore interno del telefono. Soluzioni possibili: <ul style="list-style-type: none"> • Controllare la connettività di rete. • Verificare che il server TFTP sia attivo e funzionante. • Se il server Transactional Vsam Server è installato in Cisco Unified Communications Manager, verificare che sia attivo e normalmente funzionante. • Verificare che il token di sicurezza sia valido. Eliminare manualmente i file CTL e ITL. Se le azioni precedenti non sono risultate utili, riprovare. Per ulteriori informazioni sulle Trust List, vedere la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Trust List aggiornata	Il file CTL, il file ITL o entrambi i file sono aggiornati.	Nessuna. Questo messaggio è solo informativo. Per ulteriori informazioni sulle Trust List, vedere la documentazione relativa alla versione di Cisco Unified Communications Manager in uso.
Err. versione	Il nome del file di carico del telefono non è corretto.	Verificare che il file di avvio del telefono sia corretto.

Messaggio	Descrizione	Spiegazione possibile e azione
XmlDefault.cnf.xml o .cnf.xml corrispondente al nome del telefono	Nome del file di configurazione.	Nessuna. Questo messaggio indica configurazione del telefono.

Argomenti correlati

[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

Visualizzazione della finestra Statistiche di rete

Procedura

Passaggio 1 Premere **Impostazioni > Stato > Statistiche di rete**.

Passaggio 2 Per uscire dal menu, premere **Esci**,

Campi statistiche di rete

La tabella che segue descrive le informazioni della schermata Statistiche di rete.

Tabella 23: Campi statistiche di rete

Elemento	Descrizione
Tx Frames	Numero di pacchetti inviati dal telefono.
Tx broadcast	Numero di pacchetti di trasmissione inviati dal telefono.
Tx unicast	Numero totale di pacchetti unicast trasmessi dal telefono.
Rx Frames	Numero di pacchetti ricevuti dal telefono.
Rx broadcast	Numero di pacchetti di trasmissione ricevuti dal telefono.
Rx unicast	Numero totale di pacchetti unicast ricevuti dal telefono.
ID dispositivo adiacente CDP	Identificativo di un dispositivo collegato a questa porta rilevato dal protocollo CDP.
Indirizzo IP adiacente CDP	Identificativo di un dispositivo collegato a questa porta rilevato dal protocollo CDP tramite IP.
Porta adiacente CDP	Identificativo di un dispositivo collegato a questa porta rilevato dal protocollo CDP.

Elemento	Descrizione
<p>Motivo riavvio: uno di questi valori:</p> <ul style="list-style-type: none"> • Reimpostazione hardware (reimpostazione all'accensione) • Reimpostazione software (reimpostazione anche del controller memoria) • Reimpostazione software (senza reimpostazione del controller memoria) • Reimpostazione watchdog • Inizializzato • Sconosciuto 	Causa dell'ultima reimpostazione del telefono.
Porta 1	Connessione e stato del collegamento della porta di rete (ad esempio, 100 Full significa che la porta PC è in uno stato link-up e ha autonegoziato una connessione full-duplex, 100-Mbps).
IPv4	<p>Informazioni sullo stato DHCP. Sono inclusi gli stati seguenti:</p> <ul style="list-style-type: none"> • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • DISABLED DUPLICATE IP • SET DHCP COLDBOOT • SET DHCP DISABLED • SET DHCP FAST

Elemento	Descrizione
IPv6	<p>Informazioni sullo stato DHCP. Sono inclusi gli stati seguenti:</p> <ul style="list-style-type: none"> • CDP INIT • DHCP6 BOUND • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DISABLED DUPLICATE IPV6 • DHCP6 DECLINED DUPLICATE IP • ROUTER ADVERTISE • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT CANNOT RESTORE • IPV6 STACK TURNED OFF • ROUTER ADVERTISE • ROUTER ADVERTISE • UNRECOGNIZED MANAGED BY • ILLEGAL IPV6 STATE

Visualizzazione della finestra Statistiche chiamate

Procedura

Passaggio 1 Premere **Impostazioni > Stato > Statistiche chiamate**.

Passaggio 2 Per uscire dal menu, premere **Esci**,

Campi di Statistiche chiamate

Nella tabella seguente vengono descritte le voci visualizzate nella schermata Statistiche chiamate.

Tabella 24: Voci di Statistiche chiamate

Elemento	Descrizione
Codec destinatario	Tipo di flusso vocale ricevuto (audio flusso RTP dal codec): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
Codec mitt.	Tipo di flusso vocale trasmesso (audio flusso RTP dal codec): <ul style="list-style-type: none"> • G.729 • G.722 • G.722 AMR WB • G.711 mu-law • G.711 A-law • iLBC • OPUS
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.

Elemento	Descrizione
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	
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.

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.

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



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:

- 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.
- Sul telefono, premere **Impostazioni > Informazioni di sistema**, 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:

http://<IP_address>

Pagina Web Informazioni dispositivo

L'area Informazioni dispositivo sulla pagina Web del telefono visualizza le impostazioni del dispositivo e le informazioni correlate per il telefono. La tabella che segue descrive tali voci.

Per visualizzare l'area Informazioni dispositivo, accedere alla pagina Web del telefono, quindi fare clic sul collegamento ipertestuale **Informazioni dispositivo**.

Tabella 25: Campi della pagina Web Informazioni dispositivo

Campo	Descrizione
Modalità servizio	La modalità di servizio del telefono.
Dominio servizio	Il dominio del servizio.
Stato servizio	Lo stato corrente del servizio.
Indirizzo MAC	Indirizzo MAC (Media Access Control) del telefono.
Host Name	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	Identifica la versione di installazione dell'applicazione.
ID applicazione di avvio	Indica la versione di installazione di avvio.
Versione	Identificativo del firmware in esecuzione sul telefono.
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: <ul style="list-style-type: none"> • Tipo di hardware • Nome del modello di telefono • ID prodotto • ID versione (VID): specifica il numero di versione hardware principale. • Numero di serie
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.
Mem. sistema libera	Quantità di memoria di sistema disponibile.
Memoria libera heap Java	Quantità di memoria libera per l'heap Java.

Campo	Descrizione
Memoria libera pool Java	Quantità di memoria libera per il pool Java.
Modalità FIPS abilitata	Indica se la modalità FIPS (Federal Information Processing Standard) è abilitata.

Pagina Web Impostazioni di rete

L'area di configurazione di rete sulla pagina Web di un telefono visualizza le informazioni di impostazione delle rete e sulle impostazioni di altri telefoni. 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.

Per visualizzare l'area Impostazione di rete, accedere alla pagina Web del telefono, quindi fare clic sul collegamento ipertestuale **Impostazione di rete**.

Tabella 26: Voci dell'area Impostazione di rete

Elemento	Descrizione
Indirizzo MAC	Indirizzo MAC (Media Access Control) del telefono.
Host Name	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 ottiene l'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	Indirizzo IP (Internet Protocol) del telefono.
Subnet mask	Subnet mask utilizzata dal telefono.
Router predefinito 1	Router predefinito utilizzato dal telefono.
Server DNS 1 - 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.
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.
ID VLAN operativa	VLAN (Virtual Local Area Network) operativa configurata su uno switch Cisco Catalyst a cui appartiene il telefono.
ID VLAN amministrazione	VLAN ausiliaria a cui appartiene il telefono.

Elemento	Descrizione
Unified CM 1-5	<p>Nomi host o indirizzi IP, in ordine prioritario, dei server Cisco Unified Communications Manager a cui è possibile registrare il telefono. Una voce può anche mostrare l'indirizzo IP di un router in grado di fornire funzionalità di Cisco Unified Communications Manager limitata, se tale funzionalità è disponibile.</p> <p>Per un server disponibile, una voce mostra l'indirizzo IP del server Cisco Unified Communications Manager e uno degli stati seguenti:</p> <ul style="list-style-type: none"> • Attivo: server Cisco Unified Communications Manager da cui il telefono riceve correntemente i servizi di elaborazione chiamate • In attesa: server Cisco Unified Communications Manager a cui passa il telefono se il server attuale non è più disponibile • Vuoto: nessuna connessione corrente a questo server Cisco Unified Communications Manager <p>Una voce può includere anche la designazione SRST (Survivable Remote Site Telephony), cioè un router SRST in grado di fornire funzionalità di Cisco Unified Communications Manager insieme limitato di funzioni. Questo router assume il controllo dell'elaborazione delle chiamate se gli altri server Cisco Unified Communications Manager sono irraggiungibili. Il server Cisco Unified Communications Manager di SRST viene visualizzato sempre come ultimo nell'elenco dei server se è attivo. È possibile configurare l'indirizzo del router SRST nella sezione Gruppo di server nella finestra di Cisco Unified Communications Manager Configuration.</p>
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.
Inattività URL	URL visualizzato dal telefono se è inattivo per il periodo specificato nel campo Tempo inattività URL 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 di messaggi 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 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	<p>Velocità e duplex della porta dello switch, dove:</p> <ul style="list-style-type: none"> • 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
Utente - Impostazioni internazionali	Impostazioni internazionali dell'utente associate all'utente del telefono. Identifica una serie di informazioni dettagliate per il supporto degli utenti, compresi lingua, carattere, formattazione e ora e informazioni sulla tastiera alfanumerica.
Rete - Impostazioni internazionali	Impostazioni internazionali della rete associate all'utente del telefono. Identifica una serie di informazioni dettagliate per il supporto del telefono in una ubicazione specifica, comprese definizioni di tempo e 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.
Ascolto gruppo	Indica se la funzione ascolto di gruppo è abilitata sul telefono. L'ascolto di gruppo consente di utilizzare il ricevitore e ascoltare tramite altoparlante contemporaneamente.
GARP abilitato	Indica se il telefono apprende gli indirizzi MAC dalle risposte ARP gratuite.
Selez. autom. linea abilitata	Indica se il telefono sposta la selezione alle chiamate in arrivo su tutte le linee.
DSCP per Controllo chiamate	Classificazione IP DSCP per la segnalazione del controllo delle chiamate.
DSCP per Configurazione	Classificazione IP DSCP per qualsiasi trasferimento di configurazione del telefono.
DSCP per Servizi	Classificazione IP DSCP per i servizi basati sul telefono.
Modalità Protezione	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 il telefono accetta o blocca le connessioni SSH.
CDP: porta SW	<p>Indica se il supporto CDP esiste sulla porta dello switch (abilitato per impostazione predefinita).</p> <p>Abilitare CDP sulla porta dello switch per l'assegnazione di VLAN al telefono, la negoziazione dell'alimentazione, la gestione QoS e la protezione 802.1x.</p> <p>Abilitare CDP sulla porta dello switch quando il telefono si collega a uno switch Cisco.</p> <p>Quando CDP è disabilitato in Cisco Unified Communications Manager, viene visualizzato un messaggio che indica che il CDP deve essere disabilitato sulla porta dello switch solo se il telefono si collega a uno switch non Cisco.</p> <p>I valori CDP correnti della porta dello switch e della porta PC sono visualizzati nel menu Impostazioni.</p>
LLDP-MED: porta SW	Indica se il protocollo LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery) è abilitato sulla porta dello switch.

Elemento	Descrizione
Priorità alimentazione LLDP	Indica la priorità di alimentazione del telefono allo switch, abilitando così lo switch per fornire energia ai telefoni. Le impostazioni comprendono: <ul style="list-style-type: none"> • 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	Identifica il file CTL.
File ITL	Il file ITL contiene la trust list iniziale.
Firma CTL	Ottimizza la sicurezza tramite l'algoritmo hash sicuro (SHA-1) nei file CTL e ITL.
Server CAPF	Il nome del server CAPF utilizzato dal telefono.
TVS	Il componente principale di Security by Default. Trust Verification Services (TVS) consente a Cisco Unified di autenticare i server applicazione, come i servizi EM, rubrica e MIDlet e stabilisce HTTPS.
Server TFTP	Il nome del server TFTP utilizzato dal telefono.
Sincronizzazione porta automatica	Sincronizza le porte alla velocità inferiore eliminando la perdita di pacchetti.
Configurazione remota porta switch	Consente all'amministratore di configurare velocità e funzione di porta della tabella Cisco Collaboration Experience da remoto mediante Cisco Unified Communications Manager AD.
Configurazione remota porta PC	Indica se la configurazione di porta remota della modalità velocità e duplex per la porta PC è abilitata o disabilitata.
Modalità indirizzi IP	Visualizza la modalità di indirizzamento IP disponibile sul telefono.
Control. modal. Prefer. IP	Indica la versione di indirizzo IP utilizzata dal telefono durante la segnalazione con Cisco Unified Communications Manager quando IPv4 e IPv6 sono entrambi disponibili sul telefono.
Modal. Prefer. IP per supporto	Indica che per i supporti il dispositivo utilizza un indirizzo IPv4 per collegarsi a Cisco Unified Communications Manager.
Config. automatica IPv6	Consente di visualizzare se la configurazione automatica del telefono è abilitata o disabilitata.
DAD IPv6	Verifica l'univocità dei nuovi indirizzi unicast IPv6 prima che gli indirizzi vengano assegnati alle interfacce.
Accetta messaggi reindirizzamento IPv6	Indica se il telefono accetta i messaggi di reindirizzamento dallo stesso router utilizzato per la destinazione.
Risposta richiesta echo multicast IPv6	Indica che il telefono invia un messaggio di risposta echo in risposta a un messaggio di richiesta inviato a un indirizzo IPv6.

Elemento	Descrizione
Server di caricamento IPv6	Utilizzato per ottimizzare il tempo di installazione per gli aggiornamenti del firmware del telefono scaricando la WAN memorizzando le immagini in locale, negando la necessità di attraversare il collegamento WAN per l'aggiornamento di ogni telefono.
Server di registro IPv6	Indica porta e indirizzo IP della macchina di registrazione remota a cui il telefono invia i messaggi di registro.
Server CAPF IPv6	Nome comune (da Cisco Unified Communications Manager Certificate) del CAPF utilizzato dal telefono.
DHCPv6	Il protocollo di configurazione dinamica degli indirizzi (DHCP) assegna automaticamente gli indirizzi IPv6 ai dispositivi quando vengono collegati alla rete. I telefoni IP Cisco Unified abilitano l'impostazione predefinita.
Indirizzo IPv6	Visualizza l'indirizzo IPv6 corrente del telefono o consente all'utente di specificare un nuovo indirizzo IPv6.
Lunghezza prefisso IPv6	Visualizza la lunghezza del prefisso corrente della subnet o consente all'utente di specificare una nuova lunghezza di prefisso.
Router predefinito IPv6 1	Visualizza il router predefinito utilizzato dal telefono o consente all'utente di specificare un nuovo router predefinito IPv6.
Server DNS IPv6 1	Visualizza il server DNSv6 primario utilizzato dal telefono o consente all'utente di specificare un nuovo server.
Server DNS IPv6 2	Visualizza il server DNSv6 secondario utilizzato dal telefono o consente all'utente di specificare un nuovo server DNSv6 secondario.
TFTP alternativo IPv6	Consente all'utente di abilitare l'uso di un server TFTP IPv6 alternativo (secondario).
Server TFTP IPv6 1	Visualizza il server TFTP IPv6 primario utilizzato dal telefono o consente all'utente di specificare un nuovo server TFTP primario.
Server TFTP IPv6 2	Visualizza il server TFTP IPv6 secondario utilizzato se il server TFTP IPv6 primario non è disponibile o consente all'utente di impostare un nuovo server TFTP secondario.
Indirizzo IPv6 rilasciato	Consente all'utente di rilasciare le informazioni correlate a IPv6.
Livello energia Energywise	Una misura dell'energia assorbita dai dispositivi in una rete EnergyWise.
Dominio EnergyWise	Un raggruppamento amministrativo di dispositivi con lo scopo di monitorare e controllare l'alimentazione.

Pagina Web Informazioni Ethernet

La tabella seguente descrive il contenuto della pagina Web Informazioni Ethernet.

Tabella 27: 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 Rete

Nella tabella seguente vengono descritte le informazioni contenute nelle pagine Web Area di rete.



Nota Quando si fa clic sul link **Rete** in Statistiche di rete, viene visualizzata la pagina «Informazioni porta».

Tabella 28: Voci di Area di rete

Elemento	Descrizione
Rx totalPkt	Numero totale di pacchetti ricevuti dal telefono.
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 tokenDrop	Numero totale di pacchetti abbandonati a causa di risorse insufficienti (ad esempio, overflow FIFO).
Tx totalGoodPkt	Numero totale di pacchetti corretti (multicast, broadcast e unicast) ricevuti dal telefono.
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.

Elemento	Descrizione
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.
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 IP adiacente CDP	Indirizzo IP del dispositivo adiacente rilevato dal protocollo CDP.
Indirizzo IPv6 adiacente CDP	Indirizzo IPv6 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 da LLDP.
Indirizzo IP adiacente LLDP	Indirizzo IP del dispositivo adiacente rilevato dal protocollo LLDP.
Indirizzo IP adiacente IPv6	Indirizzo IPv6 del dispositivo adiacente rilevato dal protocollo CDP.
Porta adiacente LLDP	Porta del dispositivo adiacente a cui è collegato il telefono rilevato dal protocollo LLDP.
Informazioni porta	Informazioni su velocità e duplex.

Pagine Web Registri console, Dump della memoria, Messaggi di stato e Visualizzazione debug

Sotto l'intestazione Registri dispositivi, i collegamenti ipertestuali Registri console, Dump della memoria, Messaggi di stato e Visualizzazione debug forniscono informazioni che consentono di monitorare il telefono e risolvere eventuali problemi.

- Registri console: comprende collegamenti ipertestuali ai singoli file di registro. I file di registro console comprendono messaggi di debug ed errore ricevuti dal telefono.
- Dump della memoria: comprende collegamenti ipertestuali 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. Queste informazioni vengono visualizzate anche nella schermata Messaggi di stato sul telefono.
- 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.

Pagina Web Statistiche di flusso

I telefoni IP Cisco possono trasmettere informazioni verso e da cinque 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.

Per visualizzare l'area Statistiche di flusso, accedere alla pagina Web del telefono, quindi fare clic sul collegamento ipertestuale **Flusso**.

Nella tabella seguente vengono descritte le voci delle aree Statistiche di flusso.

Tabella 29: Campi di 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 di inizio	L'indicatore di data/ora interno indica quando Cisco Unified Communications Manager ha richiesto l'inizio della trasmissione dei pacchetti da parte del telefono.
Stato flusso	Indicazione dell'eventuale attivazione del flusso.
Host Name	Nome fisso e univoco assegnato automaticamente al telefono in base all'indirizzo M
Pacchetti mittente	Numero totale di pacchetti dati RTP trasmessi dal telefono dall'avvio della connessione è 0 se la connessione è impostata sulla modalità di sola ricezione.
Otetti mitt	Numero totale di otetti di payload trasmessi dal telefono nei pacchetti dati RTP dall'a connessione. Il valore è 0 se la connessione è impostata sulla modalità di sola ricezione.
Codec mitt.	Tipo di codifica audio per il flusso di trasmissione.
Report mitt. inviati (vedere nota)	Numero di volte per cui è stato inviato il report mittente RTCP.
Ora di invio report mitt (vedere nota)	Indicazione dell'indicatore di data/ora interno relativo all'ultimo invio del rapporto RTCP.
Pacchetti persi destinatario	Numero totale di pacchetti dati RTP persi dall'avvio del ricevimento dati su questa co. Definito come il numero di pacchetti attesi meno il numero di pacchetti effettivamente ricevuti, dove il numero di pacchetti ricevuti comprende eventuali pacchetti in ritardo o duplicati. Il 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 in 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.

Elemento	Descrizione
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 dati su 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'avvio della ricezione sulla connessione. Include i pacchetti ricevuti da origini diverse, se questa chiamata è di tipo multicast. Il valore è 0 se la connessione è impostata sulla modalità di solo invio.
Indice occultamento cumulativo	Numero di frame di occultamento diviso per il numero totale di frame voce ricevuti dal flusso vocale.
Indice occultamento intervallo	Rapporto tra i frame di occultamento con 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 tre 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 di oltre il cinque per cento (frame persi) dal flusso vocale.
Latenza (vedere nota)	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.
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.
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.

Elemento	Descrizione
Ora di ricezione report destinatario (vedere nota)	Ora di ricezione più recente di un report destinatario RTCP.



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>
</CiscoIPPhoneLineInfo>
```

```

    <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 del telefono

- Informazioni generali sulla risoluzione dei problemi, a pagina 157
- Problemi di avvio, a pagina 158
- Problemi di reimpostazione del telefono, a pagina 162
- Il telefono non è in grado di connettersi alla LAN, a pagina 165
- Problemi di protezione del telefono IP Cisco, a pagina 165
- Problemi audio, a pagina 167
- Problemi generici relativi alle chiamate, a pagina 168
- Procedure di risoluzione dei problemi, a pagina 169
- Controllo delle informazioni di debug da Cisco Unified Communications Manager, a pagina 173
- Informazioni aggiuntive sulla risoluzione dei problemi, a pagina 174

Informazioni generali sulla risoluzione dei problemi

Nella tabella che segue vengono fornite informazioni generali sulla risoluzione dei problemi per il telefono IP Cisco.

Tabella 30: Risoluzione dei problemi del telefono IP Cisco

Riepilogo	Spiegazione
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 minuti) o VLAN vocale causano il ripristino dei telefoni IP, la perdita di una chiamata o l'impossibilità di avviare o rispondere a una chiamata. I telefoni possono rimanere attivi fino al termine dei disturbi di trasmissione.
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 cautela se si decide di scollegare la connessione di rete del telefono e collegare il computer desktop. Attenzione La scheda di rete nel computer non può ricevere l'alimentazione attraverso la connessione di rete; se l'alimentazione proviene dalla connessione, la scheda di rete può venire distrutta. Per spostare la scheda di rete, attendere almeno 10 secondi dopo aver scollegato il telefono prima di collegarlo al computer. Questo intervallo di tempo è sufficiente affinché lo switch rilevi l'assenza del telefono e interrompa la fornitura di energia al cavo.

Riepilogo	Spiegazione
Modifica della configurazione del telefono	<p>Per impostazione predefinita, le impostazioni della password amministratore sono bloccate per impedire agli utenti di apportare modifiche che possono influire sulla connettività di rete. Prima di poterle configurare, occorre sbloccare le impostazioni della password amministratore.</p> <p>Per informazioni, vedere Applicazione di una password al telefono, a pagina 140.</p> <p>Nota Se la password amministratore non è impostata nel profilo del telefono, l'utente può modificare le impostazioni di rete.</p>
Mancata corrispondenza del codec tra il telefono e un altro dispositivo	<p>Le statistiche RxType e TxType mostrano il codec utilizzato per una conversazione tra il telefono IP Cisco in uso e un altro dispositivo. I valori di queste statistiche devono corrispondere. In caso contrario, verificare che l'altro dispositivo possiede il codec della conversazione o che sia presente un transcoder per gestire il servizio. Per informazioni, vedere Visualizzazione della finestra Statistiche chiamate, a pagina 140.</p>
Mancata corrispondenza del campione audio tra il telefono e un altro dispositivo	<p>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 valori di queste statistiche devono corrispondere. Per informazioni, vedere Visualizzazione della finestra Statistiche chiamate, a pagina 140.</p>
Condizione di loopback	<p>Può verificarsi una condizione di loopback quando vengono soddisfatte le seguenti:</p> <ul style="list-style-type: none"> • L'opzione Configurazione porta SW del telefono è impostata su 10 Half Duplex (10-BaseT/half duplex). • Il telefono è alimentato da un alimentatore esterno. • Il telefono non è alimentato (l'alimentatore è scollegato). <p>In questo caso, la porta dello switch del telefono può disabilitarsi e il messaggio seguente viene visualizzato sul registro console dello switch:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>Per risolvere questo problema, abilitare nuovamente la porta dallo switch.</p>

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 55

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 55

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 169](#).

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. Consultare la sezione «Visualizzazione della finestra Messaggi di stato» per istruzioni sull'accesso ai messaggi di stato e un elenco dei possibili errori con relative spiegazioni e soluzioni.

Argomenti correlati

[Visualizzazione della finestra Messaggi di stato](#), a pagina 132

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 169

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.

Argomenti correlati

[Verifica delle impostazioni DHCP](#), a pagina 170

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.

Argomenti correlati

[Verifica delle impostazioni DNS](#), a pagina 172

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 172.

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.

Argomenti correlati

[Creazione di un nuovo file di configurazione del telefono](#), a pagina 171

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 62](#) 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 62](#).

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 161](#).

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.

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.

Argomenti correlati

[Verifica delle impostazioni DHCP](#), a pagina 170

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 andando a **Impostazioni** 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 170](#).

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 audio

Le sezioni seguenti descrivono come risolvere i problemi audio.

Nessun percorso audio

Problema

Una o più parti della chiamata non ricevono l'audio.

Soluzione

Quando almeno una persona che partecipa a una chiamata non riceve il segnale audio, non si è stabilita la connettività IP tra i telefoni. Verificare la configurazione dei router e degli switch per assicurarsi che la connettività IP sia configurata correttamente.

Audio disturbato

Problema

Un utente ha segnalato dei disturbi dell'audio durante le chiamate.

Causa

Potrebbe esserci una mancata corrispondenza nella configurazione jitter.

Soluzione

Controllare le statistiche AvgJtr e MaxJtr. Una notevole differenza tra queste due statistiche può indicare un problema con il jitter sulla rete o attività di rete con velocità periodica elevata.

Un telefono in modalità collegamento a cascata non funziona

Problema

In modalità collegamento a cascata, uno dei telefoni per chiamate in conferenza non funziona.

Soluzione

Verificare se i cavi collegati all'adattatore smart siano quelli corretti. I due cavi più spessi collegano i telefoni all'adattatore smart. Il cavo più sottile connette l'adattatore smart all'alimentatore.

Argomenti correlati

[Modalità collegamento a cascata](#), a pagina 33

[Installazione del telefono per chiamate in conferenza in modalità collegamento a cascata](#), a pagina 40

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.

Verifica delle impostazioni TFTP

Procedura

Passaggio 1

Verificare il campo Server TFTP 1.

Se è stato assegnato un indirizzo IP statico al telefono, è necessario immettere manualmente un'impostazione per l'opzione Server TFTP 1.

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 2 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 3 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 Spegnerne e riaccendere il telefono.

Argomenti correlati

[Individuazione dell'indirizzo MAC del telefono](#), a pagina 62

[Riavvio o reimpostazione del telefono per chiamate in conferenza](#), a pagina 175

Verifica delle impostazioni DHCP

Procedura

Passaggio 1 Sul telefono, premere **Impostazioni**.

Passaggio 2 Selezionare **Impostazioni amministratore > Configurazione Ethernet > Configurazione IPv4**.

Passaggio 3 Controllare il campo 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:

https://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

Passaggio 4

Verificare i campi Indirizzo IP, Subnet mask e Router predefinito.

Se si assegna un indirizzo IP statico al telefono, è necessario immettere manualmente le impostazioni per queste opzioni.

Passaggio 5

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:

https://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 Spegner e riaccendere il telefono.

Argomenti correlati

- [Metodi di aggiunta del telefono](#), a pagina 62
[Documentazione di Cisco Unified Communications Manager](#), a pagina 14

Verifica delle impostazioni DNS

Procedura

- Passaggio 1** Sul telefono, premere **Impostazioni**.
Passaggio 2 Selezionare **Impostazioni amministratore > Configurazione Ethernet > Configurazione IPv4**.
Passaggio 3 Verificare che il campo Server DNS 1 sia impostato correttamente.
Passaggio 4 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, EnergyWise, MobileRemoteAccess
- 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

- [Riavvio o reimpostazione del telefono per chiamate in conferenza, a pagina 175](#)
- [Monitoraggio della qualità audio, a pagina 176](#)
- [Pulizia del telefono IP Cisco, a pagina 178](#)

Riavvio o reimpostazione del telefono per chiamate in conferenza

In caso di errore, è possibile effettuare la reimpostazione di base del telefono per ripristinarlo. È inoltre possibile ripristinare le impostazioni predefinite di configurazione e protezione.

Riavvio del telefono per chiamate in conferenza

Quando si riavvia il telefono, tutte le modifiche apportate all'impostazione di rete o dell'utente non salvate nella memoria flash del telefono vengono perse.

Procedura

Premere **Impostazioni** > **Impostazioni amministratore** > **Reimposta impostazioni** > **Reimposta dispositivo**.

Argomenti correlati

[Voci di menu e di testo del telefono](#), a pagina 43

Reimpostazione delle impostazioni del telefono per chiamate in conferenza dal menu del telefono

Procedura

Passaggio 1

Premere **Impostazioni**.

Passaggio 2

Selezionare **Impostazioni amministratore** > **Reimposta impostazioni**.

Passaggio 3

Selezionare il tipo di reimpostazione.

- **Tutto:** consente di ripristinare le impostazioni di fabbrica.
- **Reimpostazione dispositivo:** reimposta il dispositivo. Le impostazioni esistenti non vengono modificate.
- **Rete:** consente di ripristinare le impostazioni predefinite della configurazione di rete.
- **Modalità servizio:** consente di cancellare la modalità di servizio corrente, disattivare la VPN e riavviare il telefono.
- **Protezione:** consente di ripristinare le impostazioni predefinite della protezione. Questa opzione elimina il file CTL.

Passaggio 4

Premere **Reimposta** o **Annulla**.

Argomenti correlati

[Voci di menu e di testo del telefono](#), a pagina 43

Ripristino delle impostazioni di fabbrica predefinite del telefono per chiamate in conferenza dalla tastiera

Quando si reimposta il telefono dalla tastiera, vengono ripristinate le impostazioni di fabbrica.

Procedura**Passaggio 1**

Scollegare il telefono:

- Se si utilizza PoE, scollegare il cavo LAN.
- Se si utilizza l'alimentatore, scollegarlo.

Passaggio 2

Attendere 5 secondi.

Passaggio 3

Tenere premuto **#** e ricollegare il telefono.

Passaggio 4

Quando il telefono si avvia, la striscia di LED si accende. Non appena si accende la striscia di LED, premere **123456789*0#** in sequenza.

Dopo aver premuto questi tasti, il telefono avvia la procedura di ripristino delle impostazioni di fabbrica.

Se non si premono i tasti in sequenza, il telefono si accende normalmente.

Attenzione Non spegnere il telefono fino al completamento della procedura di ripristino e fino alla visualizzazione della schermata principale.

Argomenti correlati

[Voci di menu e di testo del telefono](#), a pagina 43

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 31: 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.	<ul style="list-style-type: none"> • 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. <p>Controllare il numero di pacchetti trasmessi (TxCnt) e ricevuti (RxCnt) per verificare che non sia presente alcun problema nel flusso dei pacchetti voce.</p>

Modifica della metrica	Condizione
Diminuzione significativa dei punteggi MOS LQK	<p>Problema di rete derivante dalla perdita di pacchetti o da livelli di jitter elevati:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Aumento significativo dei punteggi MOS LQK	<ul style="list-style-type: none"> • 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](#), a pagina 179
- [Supporto per la registrazione delle chiamate internazionali](#), a pagina 180
- [Limitazione di lingua](#), a pagina 180

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 14

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 (Cina)
- 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** della tastiera è riportato **a b c 2 A B C**.