Installazione del telefono IP Office Platform H.323

Versione 11.1 FP2
Edizione 3
Novembre 2021

Avviso

Nonostante l'impegno profuso per garantire la completezza e la precisione delle informazioni del presente documento al momento della stampa, Avaya declina qualsiasi responsabilità per eventuali errori. Avaya si riserva il diritto di apportare cambiamenti e correzioni alle informazioni contenute nel presente documento senza alcun obbligo di notifica degli stessi a persone e a organizzazioni.

Limitazioni di responsabilità per la documentazione

Per “Documentazione” si intendono le informazioni pubblicate su diversi supporti che potrebbero includere le informazioni sul prodotto, le istruzioni d'uso e le specifiche sulle prestazioni rese generalmente disponibili agli utenti dei prodotti. Nella documentazione non sono inclusi i materiali di marketing. Avaya non è responsabile per eventuali modifiche, aggiunte o eliminazioni alla versione originariamente pubblicata della documentazione, a meno che tali modifiche, aggiunte o eliminazioni non siano state eseguite da Avaya. L'Utente finale si impegna a risarcire e a non citare Avaya, i suoi agenti, funzionari e dipendenti, in eventuali reclami, azioni legali, richieste o sentenze, derivanti o correlate a modifiche, aggiunte o eliminazioni da essi apportate a questa documentazione nei limiti di quanto effettuato.

Limitazioni di responsabilità per i link

Avaya non è responsabile del contenuto e dell'attendibilità dei siti Web cui si fa riferimento all'interno di questo sito o di questa documentazione fornita da Avaya. Avaya non è responsabile dell'accuratezza di nessuna delle informazioni, dichiarazioni o contenuti forniti su questi siti e la loro inclusione non implica l'approvazione da parte di Avaya di prodotti, servizi o informazioni contenuti o offerti negli stessi. Avaya non garantisce che tali link siano attivi e non è in grado di controllarne la disponibilità.

Garanzia

Avaya fornisce una garanzia limitata sui propri componenti hardware e software Avaya. Per conoscere le condizioni della garanzia limitata, fare riferimento al contratto di vendita. Sono, inoltre, disponibili a clienti e altre parti il testo standard della garanzia Avaya e le informazioni sull’assistenza relativa al presente prodotto nell'ambito del periodo coperto da garanzia. Per consultare questi documenti, visitare il sito Web dell'assistenza Avaya all'indirizzo: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 dal link “Warranty & Product Lifecycle” o un sito indicato successivamente da Avaya. Nota: acquistando il prodotto da un partner di canale Avaya autorizzato al di fuori dei confini degli Stati Uniti e del Canada, la garanzia viene fornita dal suddetto partner di canale e non da Avaya.

Per “**Servizio ospitato**” si intende l'abbonamento a un servizio ospitato che l'utente acquista da Avaya o da un partner di canale Avaya autorizzato (a seconda dei casi), ulteriormente descritto nella sezione SAS ospitato o nella documentazione descrittiva di altri servizi, relativa al servizio ospitato applicabile. Se si acquista un abbonamento a un Servizio ospitato, la garanzia limitata di cui sopra potrebbe non essere applicabile; tuttavia, l'utente potrebbe avere diritto a usufruire dei servizi di supporto connessi al Servizio ospitato, come illustrato più avanti nei documenti descrittivi del servizio, in relazione al Servizio ospitato applicabile. Per ulteriori informazioni, contattare Avaya o un partner di canale Avaya (a seconda dei casi).

Servizio ospitato

QUANTO SEGUE SI APPLICA SOLO IN CASO DI ACQUISTO DI UNA SOTTOSCRIZIONE A UN SERVIZIO OSPITATO DA AVAYA O DA UN PARTNER DI CANALE AVAYA (SECONDO LE CIRCOSTANZE); I TERMINI DI UTILIZZO DEI SERVIZI OSPITATI SONO DISPONIBILI SUL SITO WEB DI AVAYA, ALL'INDIRIZZO HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, IN CORRISPONDENZA DEL COLLEGAMENTO “Termini di utilizzo Avaya per i servizi ospitati” O SU ALTRI SITI INDIVIDUATI SUCCESSIVAMENTE DA AVAYA, E SONO APPLICABILI A CHIUNQUE ACCEDA AL SERVIZIO OSPITATO O NE FACCIA USO. ACCEDENDO AL SERVIZIO OSPITATO O FACENDONE USO, O AUTORIZZANDO ALTRI A FARLO, L'UTENTE, PER CONTO PROPRIO E DELL'ENTITÀ PER CUI ESEGUE TALI OPERAZIONI (DA QUI IN POI DENOMINATI IN MODO INTERSCAMBIABILE “UTENTE” E “UTENTE FINALE”), ACCETTA I TERMINI DI UTILIZZO. SE L'UTENTE ACCETTA I TERMINI DI UTILIZZO PER CONTO DI UN'AZIENDA O DI UN'ALTRA ENTITÀ LEGALE, L'UTENTE DICHIARA DI AVERE L'AUTORITÀ PER VINCOLARE TALE ENTITÀ AI PRESENTI TERMINI DI UTILIZZO. SE L'UTENTE NON DISPONE DI TALE AUTORITÀ O NON INTENDE ACCETTARE I PRESENTI TERMINI DI UTILIZZO, NON DEVE ACCEDERE AL SERVIZIO OSPITATO NÉ FARNE USO NÉ AUTORIZZARE ALCUNO AD ACCEDERE AL SERVIZIO OSPITATO O A FARNE USO.

Licenze

I TERMINI DI LICENZA DEL SOFTWARE DISPONIBILI SUL SITO WEB DI AVAYA ALL'INDIRIZZO HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO AL LINK “TERMINI DI LICENZA DEL SOFTWARE AVAYA (prodotti Avaya)”, O SU UN SITO INDICATO SUCCESSIVAMENTE DA AVAYA, SONO APPLICABILI A CHIUNQUE ABBIA SCARICATO, UTILIZZATO E/O INSTALLATO PROGRAMMI SOFTWARE AVAYA, ACQUISTATI PRESSO AVAYA INC., QUALSIASI AFFILIATO AVAYA O UN PARTNER DI CANALE AVAYA AUTORIZZATO (OVE NE RICORRA IL CASO), IN BASE A UN CONTRATTO COMMERCIALE CON AVAYA O CON UN PARTNER DI CANALE AVAYA. SALVO DIVERSAMENTE CONCORDATO DA AVAYA PER ISCRITTO, AVAYA NON ESTENDE TALE LICENZA SE IL SOFTWARE NON È STATO REPERITO DA AVAYA, DA SUOI AFFILIATI O DA UN PARTNER DI CANALE AVAYA. AVAYA SI RISERVA IL DIRITTO DI INTENTARE UN'AZIONE LEGALE CONTRO CHIUNQUE UTILIZZI O VENDA IL SOFTWARE SENZA LICENZA. INSTALLANDO, SCARICANDO O UTILIZZANDO IL SOFTWARE, O AUTORIZZANDO ALTRI A FARLO, SI ACCETTANO, PER SE STESSI E PER L'ENTITÀ PER LA QUALE SI STA INSTALLANDO, SCARICANDO O UTILIZZANDO IL SOFTWARE (DI SEGUITO “UTENTE” E “UTENTE FINALE”), TALI TERMINI E CONDIZIONI E SI CREA UN CONTRATTO VINCOLANTE CON AVAYA INC. O CON IL RELATIVO AFFILIATO AVAYA (AVAYA). O LA CONSOCIATA AVAYA APPLICABILE (“AVAYA”).

Avaya concede all'Utente una licenza secondo i termini dei tipi di licenza descritti di seguito, ad eccezione del software Heritage Nortel, il cui ambito di licenza è descritto in dettaglio di seguito. Se la documentazione dell'ordine non identifica in maniera esplicita un tipo di licenza, la licenza applicabile sarà una licenza di sistema designata come riportato nella sezione Licenza di sistema designata (DS). Il numero applicabile di licenze e di unità di capacità per le quali la licenza viene concessa è pari a uno (1), eccetto nei casi in cui venga specificato un numero diverso di licenze o di unità di capacità nella documentazione o in altri materiali a disposizione dell'Utente. Il termine “Software” indica programmi di computer in codice oggetto forniti da Avaya o da un Partner di canale Avaya sia come prodotti autonomi, preinstallati su prodotti hardware che come eventuali upgrade, aggiornamenti, patch, correzioni di errori o versioni modificate degli stessi. “Processore designato” indica un singolo dispositivo di elaborazione indipendente. Per “Server” si intende una serie di processori designati che ospita un'applicazione software accessibile da svariati utenti. Per “Istanza” si intende una singola copia del Software in esecuzione in un determinato momento: (i) su una macchina fisica; (ii) su una macchina virtuale (“VM”) con software installato o su un'installazione analoga.

Tipi di licenza

Licenza per sistema designato (DS, Designated System). L'utente finale può installare e utilizzare ciascuna copia o un'Istanza del Software esclusivamente: 1) sul numero massimo di Processori designati indicato nell'ordine o 2) sul numero massimo di Istanze del Software indicato nell'ordine, nella Documentazione o dietro autorizzazione scritta da parte di Avaya. Avaya può richiedere che i Processori designati siano identificati, nell'ordine, dal tipo, dal numero di serie, dalla codice licenza, dall'Istanza, dalla posizione o da altre designazioni specifiche o che siano forniti dall'Utente finale a Avaya attraverso mezzi elettronici stabiliti da Avaya specificatamente per questo scopo.

Licenza per utenti simultanei (CU, Concurrent User). L'utente finale può installare e utilizzare il software su più processori designati o su uno o più server a condizione che in qualsiasi momento solo il numero di unità cui è stata concessa la licenza acceda al software e lo utilizzi, secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya. Per “Unità” si intende l'unità su cui Avaya, a propria insindacabile discrezione, basa il prezzo delle licenze; può corrispondere, a titolo esemplificativo, a un agente, una porta o un utente, un account di posta elettronica o di casella vocale a nome di una persona o di un ruolo aziendale (ad esempio, webmaster o servizio di assistenza) o una voce di directory del database amministrativo utilizzato dal Software e che consente all'utente di

interagire con il Software. Le unità possono essere collegate a uno specifico Server identificato o a un'Istanza del Software.

Licenza cluster (CL). L'utente finale può installare e utilizzare ogni copia o un'istanza del software solo sul numero di cluster indicato nell'ordine o nella Documentazione, dietro autorizzazione scritta da parte di Avaya o su un (1) cluster predefinito se non indicato.

Licenza enterprise (EN). L'utente finale può installare e utilizzare ciascuna copia o un'Istanza del Software esclusivamente per l'utilizzo a livello aziendale di un numero illimitato di Istanze del Software, secondo quanto indicato nell'ordine o nella Documentazione o dietro autorizzazione scritta da parte di Avaya.

Licenza per utenti identificati (NU, Named User). L'Utente finale può: (i) installare e utilizzare ciascuna copia o Istanza del Software su un singolo Processore designato o Server per ciascun Utente identificato autorizzato (definito di seguito) o (ii) installare e utilizzare ciascuna copia o Istanza del Software su un Server a condizione che solo gli Utenti identificati autorizzati abbiano accesso al Software e lo utilizzino secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya. “Utente identificato” indica un utente o dispositivo che è stato espressamente autorizzato da Avaya ad accedere al Software e a utilizzarlo. A esclusiva discrezione di Avaya, un “Utente identificato” può essere, a titolo esemplificativo, designato per nome, funzione aziendale (ad esempio, webmaster o servizio di assistenza), account di posta elettronica o di posta vocale a nome di una persona o di una funzione aziendale oppure voce della directory del database amministrativo utilizzato dal Software che permette a un utente di interagire con il Software.

Licenza a strappo (SR, Shrinkwrap License). L'Utente finale può installare e utilizzare il Software in base ai termini e alle condizioni dei contratti di licenza pertinenti, ad esempio “a strappo” o di accettazione tramite clic (le cosiddette licenze “clickthrough”) in dotazione o relative al Software (quale la “Licenza a strappo”), secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya.

Licenza di transazione. L'utente finale può utilizzare il software per il numero massimo di Transazioni specificato entro un periodo di tempo definito e secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya. Per "Transazione" si intende l'unità su cui Avaya, a sua discrezione esclusiva, basa i prezzi della relativa licenza e può essere misurata, senza limitazioni, a seconda dell'utilizzo, dell'accesso, dell'interazione (tra client/server o cliente/organizzazione) o delle operazioni del software entro un periodo di tempo definito (ad es. ora, giorno, mese). Alcuni esempi di Transazioni includono, a titolo esemplificativo, tutti i messaggi di saluto riprodotti/messaggi di attesa abilitati, tutte le promozioni personalizzate (in qualsiasi canale), tutte le operazioni di richiamata, tutti gli agenti live o le sessioni di chat Web e tutte le chiamate instradate o reindirizzate (in qualsiasi canale). L'Utente finale non può superare il numero di Transazioni senza un previo consenso da parte di Avaya e il conseguente pagamento di un onere aggiuntivo.

Software Heritage Nortel

“Heritage Nortel Software” significa che il software è stato acquistato da Avaya come parte del suo acquisto di Nortel Enterprise Solutions nel dicembre 2009. Il Software Heritage Nortel, è il software contenuto nell'elenco dei prodotti di Heritage Nortel alla pagina http://support.avaya.com/LicenseInfo (selezionare il collegamento “Heritage Nortel Products”) o su un sito indicato successivamente da Avaya. Per il software Heritage Nortel, Avaya concede al Cliente una licenza d'uso di tale Software, la quale viene fornita in virtù del presente documento esclusivamente per il livello di attivazione o di utilizzo autorizzato, al solo scopo specificato nella Documentazione e solo per l'incorporamento o l'esecuzione in apparecchiature Avaya o la comunicazione con le stesse. Le tariffe per il software Heritage Nortel possono essere applicate in base al livello di attivazione o utilizzo autorizzato specificato in un ordine o una fattura.

Copyright

Eccetto laddove esplicitamente dichiarato, non dovrà essere fatto alcun uso del materiale presente su questo sito, della Documentazione, del Software, del Servizio ospitato o dell'Hardware forniti da Avaya. Tutti i contenuti del sito, la documentazione, i Servizi ospitati e i prodotti forniti da Avaya, comprese la selezione, la disposizione e la progettazione dei contenuti, sono proprietà di Avaya o dei relativi concessori di licenza e sono protetti dalle leggi sul copyright e sulla proprietà intellettuale, inclusi i diritti sui generis relativi alla protezione dei database. È vietato modificare, copiare, riprodurre, ripubblicare, caricare, postare, trasmettere o distribuire in qualsiasi forma qualsiasi contenuto, in tutto o in parte, incluso qualsiasi codice o software, salvo espressamente autorizzato da Avaya. La riproduzione, la trasmissione, la diffusione, la memorizzazione e/o l'utilizzo non autorizzati esplicitamente e per iscritto da Avaya sono azioni perseguibili penalmente e civilmente in base alla legislazione vigente.

Virtualizzazione

Se il prodotto viene installato in una macchina virtuale, si applica quanto segue. Ogni prodotto è dotato del proprio codice di ordinazione e dei relativi tipi di licenza. Se non diversamente specificato, ciascuna Istanza di un prodotto deve essere concessa in licenza e ordinata separatamente. Ad esempio, se il cliente dell'utente finale o il partner di canale Avaya volesse installare due istanze dello stesso tipo di prodotti, dovranno essere ordinati due prodotti di quel tipo.

Componenti di terzi

Per “Componenti di terzi” si intendono alcuni programmi software o parti incluse nel Software o nel Servizio ospitato, che potrebbero contenere software (incluso software open source) distribuito in conformità ad accordi con terzi (“Componenti di terzi”), contenenti termini relativi ai diritti d'uso di alcune parti del Software (“Termini di terze parti”). Come richiesto, le informazioni sul codice sorgente distribuito del sistema operativo Linux (pertinente ai prodotti che includono tale codice), nonché i dettagli di identificazione dei titolari di copyright relativi ai Componenti di terzi e ai relativi Termini applicabili sono disponibili nei prodotti, nella Documentazione o sul sito Web Avaya al seguente indirizzo: https://support.avaya.com/Copyright oppure su un sito indicato successivamente da Avaya. I termini di licenza del software open source forniti come Termini di terzi sono conformi ai diritti di licenza concessi nei presenti Termini di licenza del Software e possono contenere diritti aggiuntivi a vantaggio dell'Utente, come la modifica e la distribuzione del software open source. I Termini di terzi hanno la precedenza sui presenti Termini di licenza del Software esclusivamente per quanto riguarda i Componenti di terzi applicabili nella misura in cui i presenti Termini di licenza del Software impongono all'Utente restrizioni maggiori rispetto ai Termini di terzi applicabili.

Quanto riportato di seguito si applica solo se il codec H.264 (AVC) viene distribuito con il prodotto. QUESTO PRODOTTO È CONCESSO IN LICENZA IN BASE ALLA LICENZA DEL PORTAFOGLIO BREVETTI AVC PER USO PERSONALE DEL CLIENTE O ALTRI UTILIZZI SENZA SCOPO DI LUCRO, PER LE ATTIVITÀ DI (i) CODIFICA VIDEO IN CONFORMITÀ ALLO STANDARD AVC (“VIDEO AVC”) E/O (ii) DECODIFICA DI VIDEO AVC, CODIFICATI DA UN CLIENTE PER ATTIVITÀ PERSONALI E/O OTTENUTI DA UN FORNITORE DI VIDEO IN POSSESSO DI LICENZA PER LA FORNITURA DI VIDEO AVC. NESSUNA LICENZA VIENE CONCESSA O È INTESA PER QUALSIASI ALTRO UTILIZZO. POTREBBERO ESSERE DISPONIBILI ULTERIORI INFORMAZIONI FORNITE DA MPEG LA, L.L.C. VISITARE IL SITO HTTP://WWW.MPEGLA.COM.

Provider di servizi

PER I PARTNER DI CANALE AVAYA CHE OSPITANO PRODOTTI O SERVIZI AVAYA, SI APPLICA QUANTO SEGUE. IL PRODOTTO O IL SERVIZIO OSPITATO POTREBBE UTILIZZARE COMPONENTI DI TERZI SOGGETTI AI TERMINI DI QUESTI ULTIMI, PERTANTO IL FORNITORE DEL SERVIZIO DEVE OTTENERE IN MANIERA AUTONOMA UNA LICENZA DIRETTAMENTE DAL FORNITORE TERZO. I PARTNER DI CANALE AVAYA CHE OSPITANO SERVIZI AVAYA DEVONO ESSERE AUTORIZZATI DA AVAYA PER ISCRITTO E, SE TALI PRODOTTI OSPITATI UTILIZZANO O INCORPORANO DETERMINATI SOFTWARE DI TERZI, COMPRESI A TITOLO ESEMPLIFICATIVO SOFTWARE O CODEC MICROSOFT, IL PARTNER DI CANALE AVAYA DEVE OTTENERE IN MANIERA AUTONOMA QUALSIASI CONTRATTO DI LICENZA APPLICABILE A SPESE DEL MEDESIMO PARTNER DI CANALE AVAYA, DIRETTAMENTE DAL RELATIVO FORNITORE TERZO.

PER QUANTO RIGUARDA I CODEC, SE IL PARTNER DI CANALE AVAYA OSPITA PRODOTTI CHE UTILIZZANO O INTEGRANO IL CODEC H.264 O H.265, LO STESSO RICONOSCE E ACCETTA DI ESSERE RESPONSABILE PER TUTTE GLI ONERI E/O LE ROYALTY COLLEGATI. IL CODEC H.264 È CONCESSO IN LICENZA IN BASE ALLA LICENZA DEL PORTAFOGLIO BREVETTI AVC PER USO PERSONALE DEL CLIENTE O ALTRI UTILIZZI SENZA SCOPO DI LUCRO, PER LE ATTIVITÀ DI (i) CODIFICA VIDEO IN CONFORMITÀ ALLO

STANDARD AVC (“VIDEO AVC”) E/O (ii) DECODIFICA DI VIDEO AVC, CODIFICATI DA UN CLIENTE PER ATTIVITÀ PERSONALI E/O OTTENUTI DA UN FORNITORE DI VIDEO IN POSSESSO DI LICENZA PER LA FORNITURA DI VIDEO AVC. NESSUNA LICENZA VIENE CONCESSA O È INTESA PER QUALSIASI ALTRO UTILIZZO. SONO DISPONIBILI ULTERIORI INFORMAZIONI SUI CODEC H.264 (AVC) E H.265 (HEVC) DA PARTE DI MPEG LA, L.L.C. VISITARE IL SITO HTTP://WWW.MPEGLA.COM.

Conformità normativa

L'utente riconosce e accetta di essere responsabile del rispetto di leggi e regolamenti applicabili, compresi, ma non limitati a leggi e regolamenti relativi alla registrazione delle chiamate, alla privacy dei dati, alla proprietà intellettuale, al segreto commerciale, alle frodi e ai diritti di esecuzione musicale, nel paese o nel territorio dove è utilizzato il prodotto Avaya.

Prevenzione delle frodi tariffarie

“Frode telefonica” indica l'uso non autorizzato del sistema di telecomunicazione dell'utente, ad esempio da parte di persone che non sono dipendenti, agenti, subappaltatori dell'azienda o che non operano per suo conto. L'utente deve essere consapevole che il sistema potrebbe essere soggetto a rischio di frodi tariffarie che, se attuate, potrebbero far aumentare notevolmente i costi dei servizi di telecomunicazione.

Intervento di Avaya sulle frodi tariffarie

Se si ritiene di essere vittima di frode tariffaria e si necessita di assistenza o supporto tecnico, chiamare il Centro di assistenza tecnica per l'intervento contro le frodi tariffarie al numero dedicato +1-800-643-2353 per gli Stati Uniti e il Canada. Per ulteriori numeri di telefono di assistenza, visitare il sito Web dell'assistenza Avaya all'indirizzo https://support.avaya.com o un sito indicato successivamente da Avaya.

Vulnerabilità della sicurezza

Le informazioni sulle politiche di supporto alla sicurezza di Avaya sono disponibili nella sezione Security Policies and Support all'indirizzo https://support.avaya.com/security.

Le vulnerabilità sospette della sicurezza dei prodotti Avaya sono gestite per il flusso di supporto della sicurezza dei prodotti Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marchi commerciali

I marchi di fabbrica, i logo e i marchi di servizio (“Marchi”) visualizzati in questo sito, nella documentazione, nei Servizi ospitati e nei prodotti forniti da Avaya sono marchi registrati o non registrati di Avaya, delle sue consociate o di terzi. Agli utenti non è consentito l'uso di tali marchi senza previo consenso scritto di Avaya o di tali terzi eventuali proprietari del marchio. Nulla di quanto contenuto in questo sito, nella Documentazione, nei Servizi ospitati e nei prodotti garantisce, per implicazione, preclusione o in altro modo, alcuna licenza o diritto nei confronti dei Marchi, senza l'autorizzazione esplicita per iscritto di Avaya o delle terze parti applicabili.

Avaya è un marchio registrato di Avaya Inc.

Tutti i marchi di fabbrica non Avaya appartengono ai rispettivi titolari.

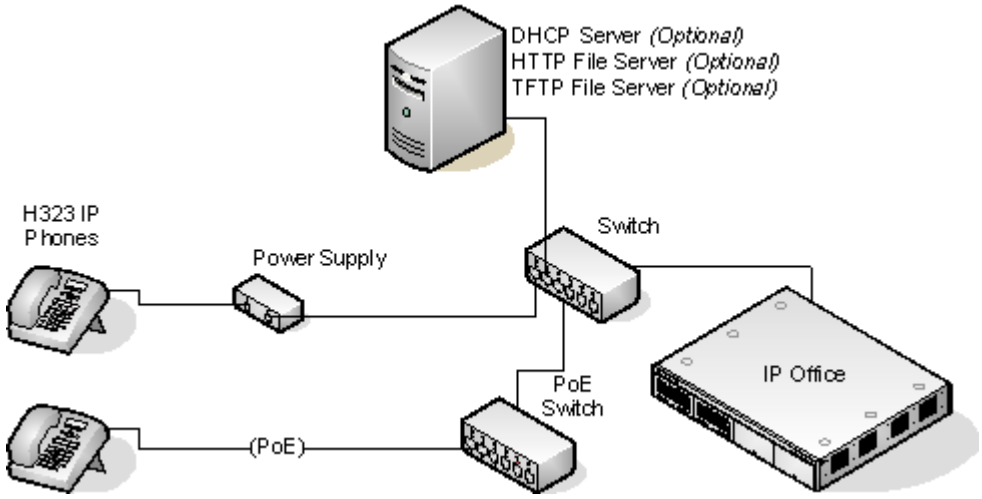
Linux® è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri Paesi.

Sommario

Parte 1: Installazione del telefono IP Office H323

Capitolo 1: Telefoni IP H.323 IP Office

La presente documentazione fornisce indicazioni per l'installazione dei telefoni IP Avaya supportati in un sistema IP Office. Va utilizzata insieme alla documentazione di installazione già esistente per tali serie di telefoni.



- **Installazione DHCP e IP Statico:** Sebbene sia possibile installare i telefoni IP H.323 con IP statico, è opportuno eseguire l'installazione con DHCP. L'uso del DHCP facilita sia il processo di installazione, che le future operazioni di manutenzione e amministrazione. Nelle installazioni statiche, a seguito di un aggiornamento del file di avvio, vengono persi tutti gli indirizzi statici ed è quindi necessario inserirli nuovamente.
- **Valutazione della rete:** La trasmissione vocale di alta qualità su rete IP richiede l'attenta valutazione di molti fattori. A tal fine:
  - Si raccomanda caldamente di far eseguire l'installazione del telefono IP solo a installatori che abbiano esperienza con il VoIP.
  - L'intera rete del cliente deve essere valutata in termini di idoneità VoIP prima dell'installazione. Avaya non supporta installazioni per le quali non siano stati forniti i risultati di una valutazione della rete. Per ulteriori dettagli, consultare Valutazione della rete alla pagina 18.

Collegamenti correlati

Novità di questa versione alla pagina 11
Telefoni IP H.323 supportati alla pagina 11
Capacità del sistema alla pagina 12
Firmware del telefono alla pagina 13
Generazione automatica dei file alla pagina 14
Installazione semplice alla pagina 14
Requisiti di installazione alla pagina 15

Novità di questa versione

Questo manuale include le seguenti modifiche introdotte nella versione IP Office 11.1:

- Funzionamento in modalità Sottoscrizione: i sistemi IP Office possono ora essere eseguiti in modalità Sottoscrizione. In questa modalità, il diritto dei telefoni IP di operare con il sistema è concesso per associazione a un utente sottoscritto, invece che a una licenza interno. La modalità Sottoscrizione supporta solo i seguenti telefoni Avaya H323:
  - Serie 1600: 1603IP/SW, 1608, 1608-I, 1616, 1616-I
  - Serie 3600: 3641, 3645
  - Serie 3700: 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Collegamento tramite stazioni base DECT R4.
  - Serie 9600: 9608, 9608G, 9611G, 9621G, 9641G, 9641GS.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Telefoni IP H.323 supportati

La presente documentazione fornisce note per l'installazione dei seguenti telefoni Avaya. Altri telefoni IP H.323 Avaya supportati, ad esempio la serie DECT R4 3700, sono trattati in una documentazione di installazione separata.

Telefoni IP H.323		Classe PoE		Porta PC	Modalità Sottoscrizione
		Classe	Inattivo		
Serie 1600	1603	2	4.4W	-	✓

La tabella continua…

Telefoni IP H.323		Classe PoE		Porta PC	Modalità Sottoscrizione
		Classe	Inattivo		
	1603SW	2	4.4W	✓	✓
	1608	2	3.7W	✓	✓
	1616	2	2.7W	✓	✓
Serie 9600	9608	1	2.08W	✓	✓
	9611G	1	2.8W	✓	✓
	9621G	2	3.49W	✓	✓
	9641G	2	3.44W	✓	✓

- 1603/1603SW - Questi telefoni richiedono un'unità di sdoppiatore PoE per poter utilizzare PoE.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Capacità del sistema

La capacità del sistema include il numero di interni del telefono configurabili e il numero di chiamate di telefoni IP simultanee.

Capacità dell'interno

Il numero massimo di telefoni IP H.323 supportati varia in base al tipo di sistema.

I sistemi IP500 V2 supportano un massimo di 384 interni. Per determinare la capacità dei telefoni IP, sottrarre il numero di porte per interni non IP fisici sul sistema, ossia il numero delle porte per interni sull'unità di controllo IP Office e sui moduli di espansione esterni. Tuttavia, tenere presente che questi sistemi supportano solo un massimo di 148 canali VCM e ciò potrebbe limitare il numero di chiamate VoIP eseguibili simultaneamente, vedere sotto.

Per i sistemi IP Office Server Edition, la capacità dell'interno IP dipende dal tipo di server. Fare riferimento al documento Avaya IP Office™ Linee guida della Piattaforma: Capacità.

Capacità chiamate

In alcuni casi il sistema IP500 V2 deve fornire un canale di compressione vocale per consentire a un telefono IP di effettuare chiamate. Questi canali sono messi a disposizione dai moduli di compressione vocale (VCM, Voice Compression Modules) installati nel sistema. Il numero di canali VCM richiesti e il tempo per il quale saranno richiesti dipende da una serie di fattori.

In sintesi:

- È richiesto un canale VCM durante la configurazione della chiamata.
- Il canale VCM è rilasciato se la chiamata è effettuata in entrata o in uscita da/verso un altro dispositivo IP che utilizza lo stesso codec di compressione (i codec VCM supportati sono G.711, G.729 e G.722).
- Il canale VCM viene utilizzato per tutta la durata della chiamata, quando la chiamata è effettuata a/da/tramite un dispositivo non IP (linea di interno o trunk).
- Tenere presente che i canali VCM vengono utilizzati anche per le chiamate da dispositivi non IP a linee IP, se configurati nel sistema IP Office (linee IP, SIP e SES).

- Le chiamate da telefoni IP al server Voicemail IP Office utilizzano un canale VCM.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Firmware del telefono

Il firmware utilizzato nei telefoni IP Avaya può essere aggiornato. Sono disponibili diverse versioni sul sito web dell'assistenza Avaya. I telefoni IP H.323 impiegati in un sistema IP Office devono tuttavia utilizzare il firmware preinstallato nel sistema IP Office o nell'applicazione IP Office Manager. Altre versioni del firmware del telefono IP potrebbero non essere state testate nello specifico con sistemi IP Office e non è pertanto opportuno utilizzarle, a meno che il supporto di IP Office non sia esplicitamente menzionato nella documentazione relativa al firmware.

Il firmware è costituito da una serie di tipi diversi di file:

Tipo di file	Descrizione
File `xxupgrade`	Il primo file richiesto da un telefono all'avvio è il file `xxupgrade`. Questo file contiene un elenco dei file con estensione bin disponibili nel set e nei numeri di versione dei file. Se la versione di un file è diversa da quella già caricata dal telefono, il telefono richiederà il nuovo file. Durante il processo, il telefono potrebbe riavviarsi in seguito al caricamento di ogni file, quindi richiedere nuovamente il file xxupgrade.txt finché non verranno caricati i firmware, se necessari. Per le varie serie di telefoni vengono forniti file distinti. Ad esempio: • `16xxupgrade.txt`: In questo file sono elencati i file del firmware che verranno caricati dai telefoni della serie 1600. • `96xxupgrade.txt`: In questo file sono elencati i file del firmware che verranno caricati dai telefoni della serie 9600. • `96x1Hupgrade.txt`: In questo file sono elencati i file firmware del che verranno caricati dai telefoni delle serie 9608, 9611, 9621 e 9641.
File `.bin`	Seguendo le istruzioni nel file `xxupgrade.txt`, il telefono caricherà eventuali file con estensione .bin richiesti, se le versioni differiscono da quelle già caricate dal telefono.
File `.tar`	Anziché i file `.bin` utilizzati da altri telefoni, i telefoni di serie 9600 utilizzano file di archivio con estensione .tar per scaricare più file in un unico passaggio, quindi li decomprimono per caricarne i contenuti.
File `46xxsettings.txt`	L'ultima riga del file `xxupgrade.txt` indica al telefono di caricare un file `46xxsettings.txt`. Si tratta di un file modificabile che è possibile utilizzare per regolare il funzionamento dei telefoni.
File `.lng`	Il firmware può includere file di lingua per l'uso con i telefoni di serie 1600 e 9600. Nel file `46xxsettings.txt` vengono impostati i file di lingua creati.

I file del firmware del telefono vengono installati nell'ambito dell'applicazione IP Office Manager e si trovano nella directory di installazione dell'applicazione. Per impostazione predefinita, la directory si trova al percorso `c:\Program Files\Avaya\IP Office\Manager`.

Gli stessi file firmware possono essere ottenuti direttamente dal pacchetto software utilizzato per installare IP Office Manager senza dover eseguire l'installazione. I file si trovano nella sottocartella `\program files\Avaya\IPOffice\Manager` della directory di installazione.

Questi set includono file con estensione bin utilizzati anche per altri dispositivi, incluso il sistema IP Office stesso.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Generazione automatica dei file

Se il sistema IP Office agisce da server dei file per i telefoni, è in grado di generare automaticamente i file `46xxsettings.txt` e .lng utilizzati dai telefoni. Questa operazione verrà eseguita se il file richiesto non è fisicamente presente nella posizione in cui il sistema archivia i file del firmware. Inoltre, il sistema utilizza le impostazioni di configurazione dell'utente per generare automaticamente i file delle impostazioni utente del telefono.

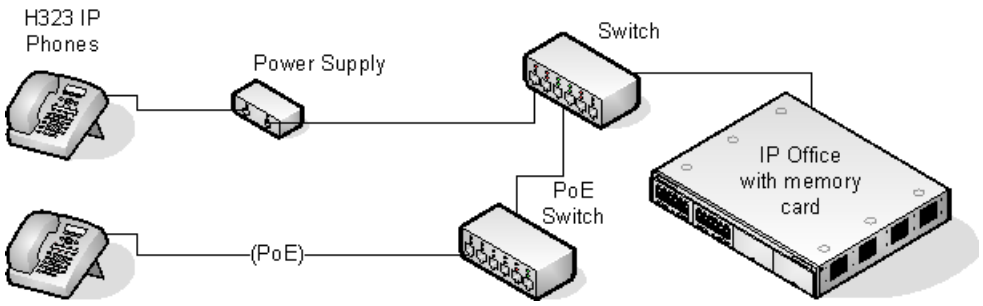
Il sistema è ancora in grado di generare automaticamente i file, anche se viene utilizzato il reindirizzamento HTTP per caricare i file `.bin` della serie 9608, 9611, 9621 e 9641 da un altro server dei file.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Installazione semplice

L'installazione più semplice prevede che il sistema IP Office funga da DHCP e file server per tutti i telefoni IP registrati.



Questo tipo di installazione usa i seguenti dispositivi:

- **Server IP Office:** Il sistema IP Office svolge diversi ruoli per i telefoni:
  - **Server DHCP:** Il sistema IP Office funge da server DHCP per i telefoni. La risposta DHCP ai telefoni include le impostazioni degli indirizzi IP, i dettagli del file server da utilizzare in base alla configurazione di IP Office e i sistemi nell'indirizzo da utilizzare come gatekeeper H.323 per i telefoni. È possibile configurare la funzione DHCP di IP Office in modo da fornire indirizzi DHCP solo in risposta a richieste da parte di telefoni

IP Avaya. Ciò consente l'utilizzo di un server DHCP alternativo per altri dispositivi che utilizzano il DHCP.

- **Gatekeeper H.323:** I telefoni IP richiedono la presenza di un gatekeeper H.323, al quale registrarsi. Il gatekeeper controlla quindi il collegamento delle chiamate in entrata e uscita dal telefono. In questo e in tutti gli scenari i sistemi IP Office fungono da Gatekeeper H.323.
- **File server:** Durante l'installazione i telefoni IP devono effettuare il download dei file firmware da un file server. A tale scopo viene utilizzato l'HTTPS, l'HTTP o il TFTP nell'ordine indicato (i telefoni delle serie 1600 e 9600 non supportano il TFTP). È possibile utilizzare la scheda di memoria dell'unità di controllo di IP Office come origine dei file.
- I sistemi IP500 V2 possono agire da server dei file per un massimo di 50 telefoni utilizzando la propria scheda di memoria. Anche i sistemi Server Edition IP Office possono agire da server dei file per un massimo di 50 telefoni. Per un numero di telefoni superiore è opportuno utilizzare un server HTTP di terze parti.
- **Server di backup/ripristino:** È possibile configurare i telefoni di serie 1600 e 9600 per eseguire il backup e il ripristino delle impostazioni utente e telefono in un server. L'indirizzo del server viene impostato separatamente rispetto a quello del file server utilizzato per il firmware del telefono, sebbene sia possibile utilizzare lo stesso server. Il metodo consigliato prevede l'utilizzo del sistema IP Office come server per questa funzione.

- **Switch:** Il sistema IP Office dispone dispone di un numero limitato di porte di connessione LAN, utilizzate al solo scopo di connettersi alla rete dati esistente. L'aggiunta di telefoni IP prevede la necessità di includere ulteriore capacità di porte.
- **Alimentatori:** È necessario che tutti i telefoni IP H.323 dispongano di un alimentatore. Il sistema IP Office non alimenta i telefoni IP. I telefoni possono essere:
  - **Alimentazione Power over Ethernet:** La maggior parte dei telefoni IP Avaya possono essere alimentati tramite un alimentatore di tipo Power over Ethernet (PoE) 802.3af. A tale scopo, utilizzare switch PoE per il supporto di più telefoni oppure singoli iniettori PoE per ogni telefono.
  - **Unità di alimentazione singole:** È possibile utilizzare un alimentatore singolo per ciascun telefono. A tal fine, è necessario avere una presa di alimentazione presso ciascun telefono. Il tipo di alimentatore varia in base al tipo di telefono. Tenere presente che i telefoni che utilizzano i moduli pulsanti potrebbero richiedere l'utilizzo di un alimentatore singolo anziché il sistema PoE.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Requisiti di installazione

Per installare un telefono IP su IP Office, sono necessari i seguenti elementi:

	Descrizione
Valutazione della rete	È necessario effettuare una valutazione della rete. Avaya non prevede il supporto VoIP in una rete per cui non sia stata eseguita una valutazione soddisfacente.
Dettagli dei numeri di interni e dei nomi utente	È richiesto un elenco completo dei dettagli dei numeri di interni e dei nomi utente previsti. Il numero dell'interno previsto non deve essere mai stato utilizzato prima e viene richiesto dal telefono durante l'installazione.
Alimentatori	Ogni telefono necessità di alimentazione. I telefoni IP Avaya non assorbono energia da IP Office. È disponibile un numero di opzioni per determinare la quantità di alimentazione erogata ai telefoni e tutti i telefoni IP Avaya supportano Power over Ethernet (PoE). Consultare Opzioni di alimentazione alla pagina 22
Presa LAN	È necessario un punto di connessione LAN Ethernet RJ45 per ogni telefono.
Cablaggio categoria	Tutti i cavi LAN e la relativa infrastruttura utilizzati con i telefoni IP H.323 devono appartenere alla categoria di cablaggio CAT5.
Cavi LAN	Controllare che in dotazione con il telefono IP sia stato fornito un cavo LAN RJ45 per il collegamento all'alimentatore. Potrebbe essere necessario un ulteriore cavo LAN RJ45 per effettuare il collegamento dall'alimentatore alla LAN del cliente, a seconda del tipo di alimentatore utilizzato. È possibile utilizzare un altro cavo LAN RJ45 per collegare il PC dell'utente alla rete LAN attraverso il telefono IP (funzionalità non supportata sui telefoni IP H.323 4601, 4602, 5601 e 5602).
Canali di compressione vocale	Per i sistemi IP500 V2, nell'unità di controllo devono essere installati i canali di compressione vocale. I canali sono richiesti durante la connessione, in caso di chiamate che coinvolgono i telefoni IP, e possono venire richiesti anche durante la chiamata. Per i dettagli completi, vedere Canali di compressione vocale alla pagina 19.
Server DHCP	L'unità IP Office può svolgere questo ruolo per tutti i telefoni. Se per la rete viene utilizzato un altro server DHCP, potrebbe fungere da DHCP per i telefoni IP H.323. Vedere Server DHCP alternativi. È inoltre possibile configurare il sistema IP Office in modo da fornire il supporto DCHP esclusivamente per i telefoni IP Avaya. • Se necessario, è inoltre possibile utilizzare un indirizzamento IP statico per l'installazione del telefono IP. Questo metodo di installazione è tuttavia sconsigliato.
File server HTTP	Un PC che esegue l'applicazione IP Office Manager può eseguire questo ruolo per un massimo di 5 telefoni IP H.323. Un'unità di controllo IP Office con una scheda di memoria può usare la scheda di memoria come origine per massimo 50 telefoni. Il sistema IP Office può fungere da file server per un massimo di 50 telefoni IP. Per un numero di telefoni superiore è opportuno utilizzare un server HTTP di terze parti.
Gatekeeper H.323	Il sistema IP Office svolge questo ruolo.
PC Manager	È necessario disporre di un PC Windows che esegue IP Office Manager per apportare modifiche alla configurazione di IP Office. Il PC deve inoltre essere dotato di System Status Application e System Monitor installati.

La tabella continua…

	Descrizione
Software del telefono IP	Il software per l'installazione del telefono IP viene installato nella cartella dei programmi dell'applicazione IP Office Manager in modo analogo a quanto accade durante l'installazione di applicazioni. È inoltre incluso nell'installazione di applicazioni IP Office Server Edition dell'applicazione IP Office nel server.
Licenze e sottoscrizioni	Per i sistemi che non vengono eseguiti in modalità di sottoscrizione, ciascun telefono IP registrato con il sistema richiede una licenza per funzionare. Sui sistemi in modalità di sottoscrizione, l'interno deve essere associato a un utente sottoscritto. Fare riferimento a Licenze e sottoscrizioni
Server di backup e ripristino	I telefoni eseguono il backup e il ripristino di varie impostazioni utente e di telefono ogni volta che l'utente esegue l'accesso o si disconnette. Vengono utilizzati file archiviati in un file server. Non si tratta necessariamente dello stesso server utilizzato per i file firmware del telefono. A tale scopo è possibile utilizzare l'archivio file del sistema IP Office (opzione consigliata).

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Licenze e sottoscrizioni

Sottoscrizioni

I sistemi che vengono eseguiti in modalità di sottoscrizione supportano un numero di interni corrispondente al numero di sottoscrizioni utenti disponibili, fino al valore massimo.

Licenze

Per i sistemi che non vengono eseguiti in modalità sottoscrizione, sono richieste licenze per ciascun interno IP.

- Nei sistemi IP Office Server Edition, l'utente deve essere configurato per un profilo utente provvisto di licenza, ad esempio una licenza utente di tipo Basic User. Gli utenti sprovvisti di licenza non possono effettuare l'accesso agli interni.
- Per i telefoni Avaya, è richiesta una licenza IP Endpoint Avaya. inclusi i telefoni di serie 1600, 9600, IP DECT, DECT R4 e Spectralink.
- Per i telefoni non-IP Avaya, è richiesta una licenza IP Endpoint di terze parti.
  - Per impostazione predefinita, la licenza viene utilizzata da ciascun telefono IP Avaya che effettua la registrazione con IP Office nell'ordine di registrazione. La licenza viene rilasciata nel momento in cui il telefono annulla la registrazione. Tuttavia, è possibile riservare le licenze per determinati telefoni per avere la certezza che tali telefoni possano disporre di una licenza in qualsiasi momento. Questa operazione si effettua mediante l'impostazione **Riserva licenza terminale Avaya IP** di ciascun interno IP. Sul sistema che utilizza le licenze WebLM, questa opzione è fissa, allo scopo di riservare una licenza.
  - I telefoni IP Avaya senza licenza possono comunque registrarsi, ma potranno essere utilizzati solo per chiamate di emergenza (chiamate con il codice funzione per le Chiamate d'Emergenza). L'utente associato risulta disconnesso e sul telefono compare il messaggio indicante che "Non sono disponibili licenze". Non appena una licenza viene resa disponibile, verrà assegnata in primo luogo a un telefono DECT sprovvisto

di licenza, quindi a qualsiasi altro telefono Avaya sprovvisto di licenza, in base all'ordine di registrazione.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10
Riserva di licenze alla pagina 35

Valutazione della rete

Il sistema IP Office è un sistema solo Voice over IP (VoIP). Tutti i trunk e gli interni si collegano al sistema tramite la rete dati del cliente. Di conseguenza, è assolutamente necessaria una valutazione della rete del cliente e, se necessario, una riconfigurazione per soddisfare le esigenze del traffico VoIP.

Avvertenza:

Durante l'installazione di telefoni IP su un sistema IP Office, Avaya presuppone che sia già stata effettuata una valutazione della rete. Se si richiede assistenza a Avaya per la risoluzione di un problema tecnico, Avaya può richiedere di consultare i risultati della valutazione della rete e, nel caso in cui i risultati della valutazione non siano soddisfacenti, potrebbe rifiutare di fornire il supporto.

L'odierna tecnologia permette di effettuare configurazioni di rete ottimali in grado di fornire servizi VoIP con una qualità vocale uguale a quella della rete telefonica pubblica. Tuttavia, solo poche reti sono configurate in modo ottimale e, di conseguenza, è necessario valutare attentamente la qualità VoIP ottenibile dalla rete di un cliente.

Non tutte le reti possono supportare le trasmissioni vocali. Alcune reti dati non hanno capacità sufficiente per il traffico vocale o presentano picchi di dati che talvolta influiscono negativamente sul traffico vocale. In oltre, l'abitudine diffusa di espandere e sviluppare le reti mediante l'integrazione di prodotti di diversi fornitori rende necessaria una verifica della compatibilità di tutti i componenti di rete con il traffico VoIP.

La valutazione della rete dovrebbe comprendere:

- Una verifica della rete finalizzata ad analizzare le apparecchiature esistenti e valutarne le capacità, compresa la capacità di soddisfare le esigenze vocali e dati attuali e future.
- La definizione degli obiettivi della rete, compresi il tipo di traffico prevalente, la scelta delle tecnologie e la definizione di obiettivi di qualità vocale.
- La valutazione deve fornire un risultato tale da garantire che la rete disporrà della capacità necessaria per il traffico dati e voce previsto.

Obiettivi della valutazione della rete

La valutazione della rete deve fornire i seguenti risultati:

- Latenza: meno di 180 ms per un ping di buona qualità. Meno di 80 ms per un ping di tipo toll quality. Si tratta della misurazione del tempo di trasferimento di pacchetti in una direzione. L'intervallo compreso fra 80 ms e 180 ms è generalmente accettabile. Tenere presente che i diversi codec audio utilizzati impongono ciascuno un ritardo fisso, causato dalla conversione dei codec qui di seguito riportata:
  - G.711: 20ms.

  - G.722: 40ms.
  - G.729: 40ms.
- Perdita di pacchetti: meno del 3% per un ping di buona qualità. Meno dell'1% per un ping di tipo toll quality. Una perdita di pacchetti eccessiva si manifesta con parole troncate e può anche causare ritardi nel setup della chiamata.
- Fluttuazione: inferiore a 20 ms. Il jitter è un'unità di misura della variazione del tempo impiegato dai diversi pacchetti di una stessa chiamata per giungere a destinazione. Un jitter eccessivo viene udito come eco.
- Durata: monitorare le statistiche una volta ogni minuto per una settimana intera. La valutazione della rete deve effettuarsi anche nel normale orario lavorativo.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Canali di compressione vocale

Le chiamate a e da apparecchi IP possono richiedere la conversione al formato codec audio utilizzato dall'apparecchio IP. Per i sistemi IP Office, questa conversione viene eseguita dai canali di compressione vocale. Questi canali supportano i comuni codec audio G.711, G.722 e G.729a.

- Per le unità di controllo IP500 V2, è possibile aggiungere i canali tramite le schede VCM IP500 e le schede combinazione IP500.
- I sistemi IP Office Server Edition forniscono i propri canali di compressione vocale tramite software e non richiedono altro hardware.

I canali di compressione vocale vengono utilizzati come segue:

Tipo di chiamata	Uso dei canali di compressione vocale
Da dispositivo IP a dispositivo non IP	Queste chiamate richiedono un canale di compressione vocale per tutta la durata della chiamata. Se non è disponibile nessun canale, la chiamata riceve segnalazione di occupato.
Da dispositivo IP a dispositivo IP	I toni di avanzamento della chiamata (ad esempio, il tono di selezione, il tono di selezione secondario, ecc.) non necessitano di canali di compressione vocale, con le seguenti eccezioni: • la conferma dei codice funzione, il campo ARS attivato e i toni di ingresso del codice account richiedono un canale di compressione vocale. Al momento della connessione di una chiamata: • Se i dispositivi IP utilizzano lo stesso codec audio, non viene usato nessun canale di compressione vocale. Se i dispositivi usano codec audio diversi, è necessario un canale di compressione vocale per ciascun dispositivo.
Da dispositivo non IP a dispositivo non IP	Nessun canale di compressione vocale richiesto.

La tabella continua…

Tipo di chiamata	Uso dei canali di compressione vocale
Musica di attesa	Viene fornita dal bus TDM di IP Office e richiede un canale di compressione vocale quando viene riprodotta su un dispositivo IP.
Risorse per conferenza e dispositivi IP	Le risorse per conferenza sono gestite dal chip conferenza, che si trova sul bus TDM di IP Office. Pertanto, è necessario un canale di compressione vocale per ciascun dispositivo IP coinvolto in una conferenza. Ciò comprende tutti i servizi che utilizzano le risorse per conferenza, come l'ascolto chiamata, l'inserimento, la registrazione della chiamata e il monitoraggio silenzioso.
Servizi Voicemail e dispositivi IP	Le chiamate ai server Voicemail di IP Office sono considerate equivalenti a chiamate dati dal bus TDM. Pertanto, le chiamate da un dispositivo IP a Voicemail richiedono un canale di compressione vocale.
Chiamate Fax	Si tratta di chiamate vocali, ma con un intervallo di frequenza leggermente più ampio delle chiamate vocali. IP Office supporta solo fax su IP tra sistemi IP Office che abbiano l'opzione di trasporto fax selezionata. Non supporta al momento i T38.
Chiamate fax T38	IP Office 5.0+ supporta le chiamate fax T38 su trunk e interni SIP. Per ciascuna chiamata fax T38, è necessario un canale VCM. Nelle reti SNC (Small Community Network) è inoltre possibile convertire una chiamata fax T38 in una attraverso le linee H.323 SCN mediante il protocollo di supporto della trasmissione di fax IP Office. Per effettuare questa conversione sono necessari 2 canali VCM. Per usare la connessione fax T38, è necessario impostare la **Classificazione delle apparecchiature** di uno degli interni analogici collegati al fax su **Dispositivo fax**. In alternativa, è anche possibile utilizzare il nuovo codice funzione **Componi fax**.

Nota:

è necessario configurare i dispositivi IP T3 per gestire pacchetti di dimensioni pari a 20 ms affinché valgano le precedenti condizioni. Se non sono configurati per pacchetti di 10 ms, è necessario un canale di compressione vocale per tutti i toni e per le chiamate a mezzi di trasmissione non diretti.

Misurazione dell'uso dei canali

È possibile utilizzare l'applicazione SSA (System Status Application) del sistema IP Office per visualizzare l'utilizzo dei canali di compressione vocale. Il numero di canali utilizzato è visualizzato nella sezione Risorse. Questa sezione indica anche per quanto tempo i canali sono risultati insufficienti e l'ultima volta che si è verificato questo evento.

Per le schede VCM IP500, il livello di utilizzo dei canali è indicato anche dai LED (da 1 a 8) presenti sul lato anteriore della scheda VCM IP500.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

QoS

Quando la voce viene trasportata tramite collegamenti a bassa velocità, è possibile che i normali pacchetti dati (pacchetti da 1500 byte) blocchino o ritardino i pacchetti vocali

(solitamente da 67 o 31 byte) sul collegamento. Ciò può danneggiare la qualità delle comunicazioni vocali.

Pertanto, è fondamentale che tutti gli switch e i router di traffico sulla rete dispongano di un meccanismo QoS (qualità del servizio). L'utilizzo di router QoS è necessario per assicurare una bassa latenza vocale e per mantenere una qualità audio sufficiente.

IP Office supporta il meccanismo QoS DiffServ (RFC2474). Questo dipende dall'utilizzo di un campo relativo al tipo di servizio (ToS) nell'intestazione del pacchetto IP. Sulle sue interfacce WAN, IP Office utilizza questo campo per impostare la priorità vocale e dei pacchetti di segnalazione vocale. Inoltre frammenta grandi pacchetti dati e, dove supportato, fornisce la compressione dell'intestazione VoIP per ridurre al minimo il sovraccarico di elaborazione WAN.

Collegamenti correlati

[Telefoni IP H.323 IP Office](#) alla pagina 10

Problemi potenziali del VoIP

È possibile che qualsiasi difetto della rete, indipendentemente dalla causa, si manifesti inizialmente con la perdita di qualità nel funzionamento del VoIP, indipendentemente dal fatto che il guasto sia relativo all'attrezzatura telefonica VoIP o meno. Pertanto, con l'installazione di una soluzione VoIP, è necessario essere consapevoli di rappresentare il primo punto di riferimento per la diagnosi e la valutazione di tutti i potenziali problemi relativi alla rete del cliente.

	Descrizione
Standard di corrispondenza end-to-end	Il VoIP dipende dal supporto e dalla selezione della stessa compressione vocale, dalla compressione dell'intestazione e dagli standard QdS in tutti gli stadi dell'indirizzamento delle chiamate. È necessario che i punti di inizio e i punti di fine utilizzino lo stesso metodo di compressione. QoS DiffServ deve essere supportato da tutti i punti intermedi.
Evitare gli hub	Gli hub producono echi e punti di congestione. Se la rete del cliente richiede connessioni LAN superiori alle capacità dell'unità IP Office stessa, è necessario utilizzare switch Ethernet. Anche se non è questo il caso, è opportuno utilizzare switch Ethernet, in quanto consentono di implementare la prioritizzazione del traffico per dispositivi VoIP.
Condizionamento, protezione e backup dell'alimentatore	I sistemi telefonici tradizionali forniscono alimentazione a tutti i dispositivi elettronici collegati a un'unica fonte. Durante un'installazione VoIP è necessario prestare a tutti i dispositivi sulla rete IP la stessa attenzione dedicata al condizionamento, alla protezione e al backup dell'alimentazione del sistema telefonico centrale.
Multidiffusione	In una rete di soli dati, è possibile che una stampante o una scheda hub non installate correttamente provochino traffico multicast senza consentire l'identificazione immediata del guasto. Il multicasting errato su una rete VoIP influirà rapidamente sulle chiamate e le funzionalità VoIP.
Indirizzo IP doppio	La duplicazione degli indirizzi è un problema frequente.

La tabella continua…

	Descrizione
Utilizzo eccessivo	È possibile che un computer che trasmette costantemente alti livelli di traffico sovraccarichi una rete, provocando la scomparsa del servizio VoIP.
Accesso alla rete	Una rete IP è molto più aperta alla connessione di un nuovo dispositivo o all'installazione di software su dispositivi esistenti che in seguito influenzano il VoIP.
Cavi di collegamento	Tecnicamente il VoIP è in grado, larghezza di banda permettendo, di funzionare su qualsiasi collegamento di rete IP. In pratica, sono fondamentali i cavi Cat5.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Collegamento al PC dell'utente

Per semplificare il numero di collegamenti LAN dalla postazione dell'utente, è possibile instradare il cavo LAN Ethernet del PC attraverso la maggior parte dei telefoni IP Avaya.

Il cavo LAN deve essere collegato dal PC alla presa con il simbolo del PC ( ) sul retro del telefono IP. Non è necessario modificare la configurazione di rete del PC precedentemente utilizzata per il collegamento diretto alla LAN. La porta supporta le connessioni Ethernet a 10/100 Mbps. I telefoni con un suffisso G supportano anche le connessioni Gigabit a 1000 Mbps.

Per i telefoni sprovvisti di una porta PC è necessario utilizzare un adattatore Gigabit (SAP 700416985) a parte. Questo apparecchio consente di dividere il traffico dati e vocale prima che questo raggiunga il telefono, con un output di 10/100 Mbps per il telefono e di 10/100/1000 Mbps per il PC. L'adattore utilizza l'alimentazione esistente del telefono. Consultare il documento "*Installazione adattatore Ethernet Gigabit e istruzioni di sicurezza*" (16-601543).

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Opzioni di alimentazione

È necessario che tutti i telefoni IP H.323 dispongano di un alimentatore. in quanto non vengono alimentati dal sistema telefonico. Di seguito vengono elencate le opzioni di alimentazione utilizzabili.

Lo standard IEEE 802.3af è più comunemente conosciuto come Power over Ethernet (PoE). Questo standard consente ai dispositivi di rete di ricevere alimentazione attraverso il cavo di rete utilizzando gli stessi fili dei segnali dati. Tutti i telefoni IP H.323 Avaya supportati in IP Office supportano anche questo standard.

Se viene installato un numero elevato di telefoni, è consigliabile utilizzare switch PoE. In altri scenari è possibile utilizzare singoli iniettori PoE per aggiungere supporto di alimentazione PoE alla connessione LAN del telefono da uno switch non- PoE.

Telefoni IP H.323	Modelli supportati	Classe PoE 802.3af	
		Classe	Inattivo
Serie 1600	1603	2	4.4W
	1603W	2	4.4W
	1608	2	3.7W
	1616	2	2.7W
Serie 9600	9608	1	2.08W
	9611G	1	2.8W
	9621G	2	3.49W
	9641G	2	3.44W

I telefoni 1603 e 1603SW richiedono un'unità di sdoppiatore PoE a parte per poter utilizzare PoE.

Il superamento del limite di classe di una porta PoE o del supporto di classe totale di uno switch PoE può provocare errori di funzionamento.

Tenere presente che i requisiti di alimentazione sono maggiori per i telefoni in uso con moduli tasti aggiuntivi e altri accessori. Per i telefoni 9608, 9611, 9621 e 9641, impostare l'interruttore di alimentazione del telefono su H e considerare l'apparecchio come appartenente alla Classe 3.

Telefoni serie 1600

Questi telefoni possono utilizzare PoE (come sopra) oppure gli alimentatori con spina situata sul lato superiore dei telefoni di serie 1600. Sono disponibili vari modelli di alimentatori di questo tipo per i diversi tipi di prese di alimentazione locali. L'alimentatore si collega al telefono mediante un connettore cilindrico sotto il telefono.

Telefoni 9608, 9611, 9621 e 9641

Questi telefoni supportano solo un connettore PoE (Power over Ethernet). Se non sono forniti con uno switch PoE, è possibile utilizzare un iniettore PoE a porta singola Avaya Global per ciascun telefono.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Opzioni del file server

Durante l'installazione e la manutenzione, i telefoni effettuano il download di vari file firmware. A tal fine, il telefono richiede in primo luogo i file per un server HTTPS. Se non riceve risposta, cercherà di ottenere i file da un server HTTP. L'indirizzo del server da utilizzare viene fornito all'interno della risposta DHCP ricevuta dal telefono da parte del server DHCP. Se il sistema IP Office viene utilizzato come server DHCP, l'indirizzo del file server viene impostato nell'ambito della configurazione di IP Office. Per i telefoni installati mediante indirizzi statici, l'indirizzo del file server corrisponde a uno degli indirizzi immessi durante l'installazione.

- Ogni telefono tenterà di richiedere file dal file server a ogni riavvio. Se tuttavia il telefono non riceve risposta, continuerà a eseguire il riavvio con i file esistenti all'interno della

memoria. Non esiste pertanto alcun requisito perché il file server sia sempre disponibile dopo l'installazione.

- I telefoni utilizzano inoltre un server per le operazioni di backup e ripristino delle impostazioni utente durante l'utilizzo del telefono. L'indirizzo di questo server viene definito da un set di indirizzi separati nel file `46xxsettings.txt`. Non si tratta necessariamente dello stesso server utilizzato per il firmware del telefono. Tuttavia, per il funzionamento di IP Office, è consigliabile utilizzare l'indirizzo del server IP Office come file server di backup e ripristino.

Per il file server dei telefoni IP installati in un sistema IP Office, sono disponibili le opzioni indicate di seguito.

Server del file	**Fino ai telefoni X**	**TFTP (Porta 69)**	**HTTP (Porta 80)**	**HTTPS (Porta 411)**
IP Office Manager Se in esecuzione,IP Office Manager può fungere da server HTTP/TFTP per richieste di file dai telefoni IP.	5	✓	✓	-
Scheda di memoria IP500 V2 Per le unità di controllo IP Office dotate di una scheda di memoria, la scheda in questione può essere usata per fornire i file software. Per le unità di controllo IP500 V2 la scheda SD di sistema è un elemento essenziale e viene precaricata con i file firmware del telefono durante la creazione e gli aggiornamenti del telefono. Diversi altri file possono essere generati automaticamente tramite IP Office, se non presenti nella scheda di memoria.	50	✓	✓	✓
IP Office Server Edition/IP Office Select Per i sistemi IP Office, l'applicazione IP Office può agire da server dei file. I file del firmware del telefono vengono installati nel server durante l'installazione di IP Office. Diversi altri file possono essere generati automaticamente tramite IP Office, se non presenti nella scheda di memoria.	[1]	-	✓	✓
Software di terze parti Il software del file server HTTP e TFTP di terze parti è disponibile attraverso molte origini, tra cui Avaya.	-	✓	✓	✓

[1] All'interno di una rete Selezionare IP Office Server Edition/IP Office, i server (diversi dall'espansione IP500 V2) possono fungere da server dei file in caso di capacità completa dei telefoni. Tuttavia, la frequenza supportata per l'aggiornamento del firmware dipende dal tipo di server, come indicato qui di seguito. Se sono necessarie prestazioni di aggiornamento superiori a questi valori, è possibile utilizzare un server dei file HTTP/S esterno.

- Dell R240: 100 telefoni per 50 minuti.

- HP DL360G7: 200 telefoni per 50 minuti.
- Dell R640: 300 telefoni per 50 minuti.
- OVA: Fino a 300 telefoni per 50 minuti.

[2] Per la versione 9.0 IP Office e per i sistemi IP Office che agiscono da server dei file, è possibile applicare il reindirizzamento HTTP al fine di reindirizzare a un server HTTP separato le richieste di file .bin da parte del telefono della serie 9608, 9611, 9621 e 9641.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Schede di memoria dell'unità di controllo

La scheda di memoria utilizzata con i sistemi IP500 V2 può essere utilizzata per archiviare i file, inclusi quelli utilizzati dai telefoni IP Avaya.

L'unità di controllo IP500 V2 richiede sempre una scheda SD di sistema. In fase di creazione, nella scheda viene aggiunto un set completo di file firmware di IP Office, inclusi i file utilizzati dai telefoni IP Avaya.

Test del server dei file

È possibile utilizzare un browser Web per eseguire un test di base del server dei file. Ad esempio, se si utilizza il protocollo HTTP, immettendo `http://<server_address>/46xxsettings.txt` si dovrebbe visualizzare il file `46xxsettings.txt`.

Se si utilizza il sistema IP Office per la generazione automatica dei file, il file delle impostazioni include una porzione di testo che indica la generazione automatica da parte del sistema in risposta alla richiesta del file. Ciò è utile non solo per controllare il funzionamento del server dei file, ma anche per visualizzare le impostazioni fornite dal sistema IP Office.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Richieste di File da parte del Telefono

Quando vengono avviati, la maggior parte dei telefoni IP Avaya richiede diversi file da un server del file:

1. generalmente, questo processo comincia con la richiesta di un file di upgrade. Tale file indica il firmware che il telefono deve eseguire. Se risulta diverso dal firmware in esecuzione, il telefono aggiunge i file software elencati a quelli che scaricherà. L'ultima riga del file di upgrade indica il nome del file di impostazioni che dovrebbe richiedere.
2. Il telefono richiede un file. che passa un elevato numero di impostazioni di configurazione al telefono. Sono inoltre indicati ulteriori file che il telefono dovrebbe richiedere, come i file delle lingue e gli screensaver.

3. Il telefono richiede file aggiuntivi:
   - Tutti i file firmware indicati nel file di upgrade.
   - Tutti gli altri file indicati nel file di impostazioni.
   - Tutti gli altri file di impostazioni.
4. Il telefono può inoltre richiedere un file di impostazioni utente.

Quello riportato qui sopra è solo un riepilogo generale. In base al telefono, l'ordine di richiesta dei file può variare. Inoltre, se richiede il firmware per un upgrade, il telefono potrebbe interrompere la richiesta di file fino al termine dell'upgrade e il riavvio del telefono.

Quando il sistema IP Office viene utilizzato come server del file, può generare automaticamente molti dei file richiesti dal telefono.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10
Generazione automatica dei file alla pagina 26

Generazione automatica dei file

Quando vengono riavviati, i telefoni IP Avaya richiedono diversi file dal file server. Ad esempio i file di configurazione del telefono e del firmware.

Quando si utilizza il sistema IP Office come file server e il telefono richiede un file, se quel file non è disponibile, il sistema potrebbe autogenerarne uno. Il file generato automaticamente utilizzerà una combinazione di impostazioni e opzioni predefinite dalla configurazione del sistema. Una volta fornito al telefono richiedente, il file generato automaticamente non verrà conservato nel sistema.

Questa funzione si applica alla maggior parte dei tipi di file eccetto ai file firmware effettivi (esempio `.bin`, `.zip`, `.tar`) e ai file certificati. Se un file appropriato viene caricato nel sistema, la generazione automatica di quel file viene saltata.

Nel file `46xxsettings.txt` generato automaticamente:

- Le impostazioni che si basano sulle voci di configurazione di IP Office, ad esempio le impostazioni sulla lingua, sono visualizzate nelle sezioni denominate "AUTOGENERATEDSETTINGS".
- Le impostazioni che rimangono invariate per tutti i sistemi IP Office con la stessa versione del software sono visualizzate nella sezione denominata "NONAUTOGENERATEDSETTINGS".

Test del server dei file

È possibile utilizzare un browser Web per eseguire un test di base del server dei file. Ad esempio, se si utilizza il protocollo HTTP, immettendo `http://<server_address>/46xxsettings.txt` si dovrebbe visualizzare il file `46xxsettings.txt`.

Se si utilizza il sistema IP Office per la generazione automatica dei file, il file delle impostazioni include una porzione di testo che indica la generazione automatica da parte del sistema in risposta alla richiesta del file. Ciò è utile non solo per controllare il funzionamento del server dei file, ma anche per visualizzare le impostazioni fornite dal sistema IP Office.

Collegamenti correlati

Richieste di File da parte del Telefono alla pagina 25

Scheda di memoria dell'unità di controllo

La scheda di memoria utilizzata con i sistemi IP500 V2 può essere utilizzata per archiviare i file, inclusi quelli utilizzati dai telefoni IP Avaya.

L'unità di controllo IP500 V2 richiede sempre una scheda SD di sistema. In fase di creazione della scheda usando IP Office Manager, nella scheda viene aggiunto un set completo di file firmware di IP Office, inclusi i file utilizzati dai telefoni IP Avaya.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Aggiunta della registrazione all'elenco indirizzi disabilitati

Il sistema IP Office registra le richieste di registrazione H.323/SIP non riuscite. Più tentativi non riusciti possono determinare il blocco dell'interno e/o dell'indirizzo IP per un periodo di tempo.

Il blocco si applica nel modo seguente:

Metodo	Descrizione
Blocco degli interni	I tentativi di registrazione in un interno esistente tramite una password sbagliata vengono bloccati per 10 minuti dopo 5 tentativi non riusciti in un periodo di 10 minuti.
Blocco degli indirizzi IP	I tentativi di registrazione in un interno non esistente o tramite una password sbagliata di un interno esistente vengono bloccati per 10 minuti dopo 10 tentativi non riusciti in un periodo di 10 minuti.

Quando si verifica un blocco, il sistema genera un allarme in System Status Application e aggiunge una voce al registro di controllo. Inoltre, viene generato un allarme di sistema, che può essere emesso tramite uno degli instradamenti degli allarmi di sistema supportati (SMTP, SNMP, Syslog).

System Monitor è in grado di visualizzare i dettagli degli indirizzi IP e degli interni disabilitati, selezionare **Stato** > **Indirizzi IP inseriti nella blacklist e stato** > **Interni disabilitati**.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Blocco dei passcode predefiniti

Informazioni su questa attività

Per IP Office versione 11.0 e successive, le impostazioni di sicurezza predefinite bloccano l'utilizzo delle password telefoniche predefinite, ad esempio 0000, per la registrazione degli interni.

Procedura

1. Tramite IP Office Manager, accedere alla configurazione di sicurezza del sistema.
2. Nella scheda **Generale**, deselezionare la casella di controllo **Blocca codici di accesso telefoni IP predefiniti**.
3. Salvare le impostazioni.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10

Capitolo 2: Impostazioni telefono aggiuntive

I file di impostazioni `46xxsettings.txt` generati automaticamente sono adatti alla maggior parte delle installazioni. Tuttavia, in alcuni scenari potrebbe essere necessario modificare il valore delle impostazioni nel file o aggiungere ulteriori impostazioni. Questo obiettivo può essere raggiunto in più modi:

- **Utilizzo di file statici:** sostituire il file generato automaticamente con un file effettivo. Questo metodo è consigliato solo per gli utenti esperti nella modifica dei file di impostazioni dei telefoni Avaya. Lo svantaggio principale è che non sarà possibile sfruttare la modifica automatica delle impostazioni affinché corrispondano alle modifiche nella configurazione di IP Office. Consultare Configurazione e modifica delle impostazioni dei file alla pagina 31.
- **Utilizzare un file di impostazioni:** Se nel sistema è presente un file chiamato `46xxsettings.txt`, il file `46xxsettings.txt` generato automaticamente indica al telefono di richiedere tale file. Ciò consente all'utente di caricare un file speciale che contiene impostazioni aggiuntive o che ignora le impostazioni selezionate nel file generato automaticamente. Consultare 46xxspecials.txt alla pagina 30.
- **Utilizza numeri origine NoUser:** diverse impostazioni del numero origine NoUser possono essere utilizzate per aggiungere valori speciali al file di impostazioni generato automaticamente. Consultare NoUser Source Numbers alla pagina 31.

Comandi comuni aggiuntivi

Qui di seguito sono indicati alcuni comandi aggiuntivi utilizzati di frequente. Per informazioni complete sui comandi disponibili, fare riferimento al manuale dell'amministratore Avaya corrispondente alla serie di telefoni specifica.

Descrizione	Impostazione del comando file
Password/CRAFT Consente di impostare l'elemento PROCPSWD specificato nel file `46xxsettings.txt` generato automaticamente, in cui X rappresenta la password. Ciò è utile per l'utilizzo di TLS, che non è possibile abilitare nei telefoni in cui PROCPSWD è impostato come valore predefinito.	`SET PROCPSWD X`
Password amministratore Consente di impostare la password dell'amministratore del telefono Vantage specificata nel file `46xxsettings.txt` generato automaticamente, in cui X rappresenta la password.	`SET ADMIN_PASSWORD X`

La tabella continua…

Descrizione	Impostazione del comando file
Funzionamento della cuffia Per impostazione predefinita, le cuffie del telefono vengono riagganciate quando l'altra parte si disconnette. L'impostazione di questo numero di origine modifica tale comportamento, in modo che le cuffie rimangano sganciate quando l'altra parte si disconnette.	`SET HEADSYS 1`
Timer di retroilluminazione Consente di impostare il timer della retroilluminazione del telefono in minuti.	`SET BAKLIGHTOFF 60`

Screensaver
Questo set di comandi
1. Abilita screensaver
2. Impostare il nome dello screensaver da scaricare
3. Consente di impostare il nome del file scaricato attuale da utilizzare.
	`SET SCREENSAVERON`
	`SET SCREENSAVER_IMAGE J179scr_svr.jpg`
	`SET SCREENSAVER_IMAGE_DISPLAY J179scr_svr`

Immagine di sfondo Questo set di comandi 1. Impostare il nome dell'immagine di sfondo da scaricare 2. Il nome del file scaricato attuale da utilizzare.	`SET BACKGROUND_IMAGE J179bck_grnd.jpg` `SET BACKGROUND_IMAGE_DISPLAY J179bck_grnd`

Vi sono diversi numeri utente NoUser utilizzati per l'interno remoto. La differenza sta nel fatto che i valori esistenti nel file di impostazioni generato automaticamente vengono modificati quando il sistema rileva che il telefono che richiede il file è un interno remoto. Consultare il manuale *"Telefoni SIP di IP Office con ABSCE"*.

Collegamenti correlati

46xxspecials.txt alla pagina 30
NoUser Source Numbers alla pagina 31
Configurazione e modifica delle impostazioni dei file alla pagina 31

46xxspecials.txt

Per i sistemi che utilizzano il file 46xxsettings.txt generato automaticamente, uno dei modi per aggiungere ulteriori impostazioni manuali è quello di utilizzare un file chiamato `46xxspecials.txt`. Quando si aggiunge questo file al sistema, il comando **`GET 46xxspecials.txt`** viene visualizzato come ultima riga del file `46xxspecials.txt` generato automaticamente e richiesto dai telefoni.

Il file `46xxspecials.txt` deve essere creato manualmente e aggiunto al file server del telefono. Può essere:

- Un file di testo semplice contenente un unico comando
- Un file di impostazioni complesso con impostazioni basate sul tipo di telefono, modello, gruppo, o modello e gruppo

Per un esempio di struttura complessa, navigare su `http://<IPOffice>/46xxspecials.txt` e ottenere un file generato automaticamente. Salvare e modificare il file prima di caricarlo nuovamente nel sistema.

Collegamenti correlati

Impostazioni telefono aggiuntive alla pagina 29

NoUser Source Numbers

Most values in the auto-generated settings file are based on settings taken from the IP Office system configuration. However, it may occasionally be necessary to add additional values to the auto-generated files. This can be done using the values entered as `NoUser` source numbers.

- Since these changes are applied to the values in the auto-generated `46xxsettings.txt` file, they are overridden by any setting entered in the `46xxsettings.txt` file if present.
- There are a number of **NoUser** source number settings used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. Refer to the IP Office SIP Phones with ASBCE manual.

Example NoUser Source Numbers

	Description
`SET_46xx_PROCPSWD=X`	This NoUser source number adds the command **`SET PROCPSWD X`** to the auto-generated settings file where **`X`** is the password set.
`SET_ADMINPSWD=X`	This NoUser source number adds the command **`SET ADMINPSWD X`** to the auto-generated settings file where **`X`** is the password set.
`SET_HEADSYS_1`	This NoUser source number adds the command **`SET ADMINPSWD X`** to the auto-generated settings file.
`SET_BAKLIGHTOFF=N`	This NoUser source number adds the command **`SET BAKLIGHTOFF N`** to the auto-generated settings file provided to a remote extension. **`N`** is the timeout in minutes.

Related links

Impostazioni telefono aggiuntive on page 29

Configurazione e modifica delle impostazioni dei file

Informazioni su questa attività

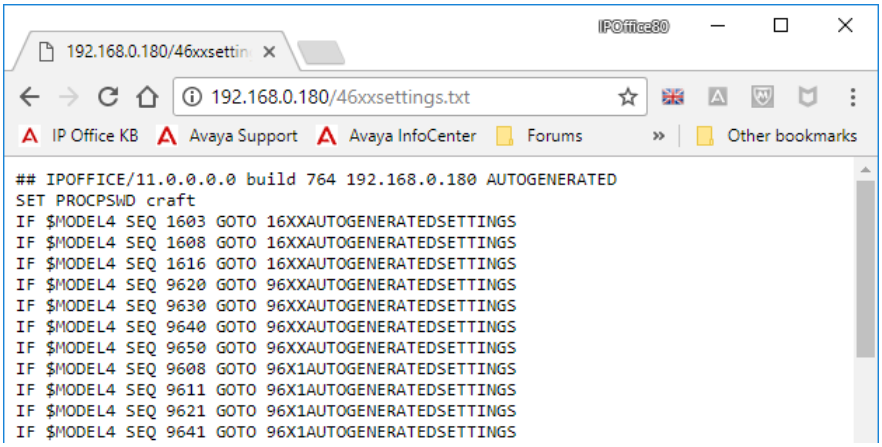
La maggior parte dei telefoni IP Avaya scarica un file delle impostazioni al riavvio.

Nota:

Ove possibile, utilizzare il sistema IP Office come file server e consentire che generi automaticamente i file di impostazioni. Ciò è utile poiché il sistema modifica automaticamente le impostazioni fornite ai telefoni affinché corrispondano alle modifiche apportate alla configurazione del sistema.

Procedura

1. Accedere al sistema e immettere il nome del file delle impostazioni del telefono specifico richiesto, ad esempio http://192.168.42.1/46xxsettings.txt. Il file generato automaticamente viene visualizzato nel browser.



   - La maggior parte dei telefoni: `46xxsettings.txt`
   - Serie 1100/1200: `11xxsettings.txt`
   - H175: `H1xxsettings.txt`

2. Salvarlo come file di testo locale.
   - Per salvare il file utilizzando il browser Chrome, fare clic con il tasto destro sulla finestra e selezionare **Salva con nome**.
   - Per salvare il file utilizzando il browser Explorer, selezionare **File** > **Salva con nome**.
   - Per salvare il file utilizzando il browser Firefox, selezionare **Salva pagina con nome**.

   A questo punto, è possibile modificare il file scaricato con un editor di testo. I campi supportati vengono descritti nei manuali di amministrazione appropriati per le varie serie dei telefoni.
3. Al termine dell'operazione, caricare il file nel server dei file in uso da parte dei telefoni.
4. Riavviare il telefono o i telefoni affinché ricarichino i propri file, compreso il download del file delle impostazioni modificato.

Collegamenti correlati

Impostazioni telefono aggiuntive alla pagina 29

Parte 2: Procedura di installazione di base

Installazione del telefono IP H.323

Di seguito è indicato un riepilogo dei passaggi principali del processo di installazione. Il metodo di installazione consigliato è quello di utilizzare DHCP, ove possibile, il sistema IP Office come file server e di abilitare la creazione automatica di utenti e interni.

	Descrizione
PC Manager:	Verificare che IP Office Manager, System Status Application e System Monitor siano installati e possano essere utilizzati per connettersi al sistema IP Office. Verificare di essere in grado di ricevere la configurazione dal sistema e di reinviarla.
Canali di compressione vocale	Per i sistemi IP500 V2, nell'unità di controllo devono essere installati i canali di compressione vocale. Utilizzare System Status Application (SSA) o in alternativa l'applicazione System Monitor per verificare che i canali di compressione vocale siano disponibili. SSA elenca i canali dei moduli di compressione vocale (VCM) sullo schermo **Risorse**. Le prime righe dell'output di Monitor includono la voce VCOMP=, che indica il numero di canali installati nell'unità di controllo.
Licenze o sottoscrizioni	A seconda della modalità operativa del sistema, ciascun telefono richiede una licenza o una sottoscrizione. È possibile registrare i telefoni senza una licenza o una sottoscrizione, ma non sarà possibile utilizzarli. Consultare Licenze e sottoscrizioni alla pagina 17.
Impostazioni del gatekeeper H	Nel sistema IP Office è abilitato per impostazione predefinita il supporto per i telefoni H.323. Ciò nonostante, è necessario controllare l'impostazione.
Impostazione del server DHCP	DHCP è il metodo consigliato per l'installazione di telefoni IP in un sistema IP Office. Il metodo prevede che sia configurato un server DHCP per il supporto dei telefoni IP. A tale scopo è possibile utilizzare il sistema IP Office. Se il cliente desidera utilizzare il proprio server DHCP, è necessaria una configurazione aggiuntiva.
Impostazione del server del file del telefono	Se per DHCP viene utilizzato il sistema IP Office, dovrà essere configurato con l'indirizzo del server del file. Indipendentemente dal metodo di installazione e dal file server selezionati, è necessario aggiungere i file firmware del telefono ai file disponibili nel server.

La tabella continua…

	Descrizione
Impostazioni interno e utente	È possibile configurare il sistema IP Office in modo che vengano create automaticamente voci utente e interno nella configurazione di ciascun telefono IP installato. Se non si utilizza la creazione automatica, sarà necessario creare manualmente le voci per ogni interno e utente prima di installare i telefoni.
Collegamenti del telefono	Una volta completati i passaggi indicati, sarà possibile collegare i telefoni alla rete. In caso di utilizzo di DHCP, i telefoni otterranno automaticamente le informazioni sull'indirizzo IP e altre impostazioni, quindi inizieranno a caricare i file. Se non si utilizza DHCP, sarà necessario eseguire il processo manuale di immissione delle informazioni sull'indirizzo IP e delle altre impostazioni.
Registrazione telefono	Dopo che i telefoni avranno scaricato tutti i file necessari dal server del file, tenteranno di effettuare la registrazione al sistema IP Office. I telefoni richiederanno l'immissione del numero di interno da utilizzare in futuro.
Test	È consigliabile testare il funzionamento dei telefoni effettuano una serie di chiamate, incluse chiamate a interni.
Postinstallazione	Se è stata utilizzata la creazione automatica per le voci di interno e/o utente, è opportuno disabilitare queste impostazioni in seguito all'installazione di tutti i telefoni. In questo manuale verrà analizzata esclusivamente la configurazione utente di base necessaria per l'installazione. Sarà ora possibile configurare completamente i nuovi utenti per soddisfare le esigenze dei clienti.

Capitolo 3: Licenze e sottoscrizioni

Sottoscrizioni

I sistemi che vengono eseguiti in modalità di sottoscrizione supportano un numero di interni corrispondente al numero di sottoscrizioni utenti disponibili, fino al valore massimo.

Licenze

Per i sistemi che non vengono eseguiti in modalità sottoscrizione, sono richieste licenze per ciascun interno IP.

- Nei sistemi IP Office Server Edition, l'utente deve essere configurato per un profilo utente provvisto di licenza, ad esempio una licenza utente di tipo Basic User. Gli utenti sprovvisti di licenza non possono effettuare l'accesso agli interni.
- Per i telefoni Avaya, è richiesta una licenza IP Endpoint Avaya. inclusi i telefoni di serie 1600, 9600, IP DECT, DECT R4 e Spectralink.
- Per i telefoni non-IP Avaya, è richiesta una licenza IP Endpoint di terze parti.
  - Per impostazione predefinita, la licenza viene utilizzata da ciascun telefono IP Avaya che effettua la registrazione con IP Office nell'ordine di registrazione. La licenza viene rilasciata nel momento in cui il telefono annulla la registrazione. Tuttavia, è possibile riservare le licenze per determinati telefoni per avere la certezza che tali telefoni possano disporre di una licenza in qualsiasi momento. Questa operazione si effettua mediante l'impostazione **Riserva licenza terminale Avaya IP** di ciascun interno IP. Sul sistema che utilizza le licenze WebLM, questa opzione è fissa, allo scopo di riservare una licenza.
  - I telefoni IP Avaya senza licenza possono comunque registrarsi, ma potranno essere utilizzati solo per chiamate di emergenza (chiamate con il codice funzione per le Chiamate d'Emergenza). L'utente associato risulta disconnesso e sul telefono compare il messaggio indicante che "Non sono disponibili licenze". Non appena una licenza viene resa disponibile, verrà assegnata in primo luogo a un telefono DECT sprovvisto di licenza, quindi a qualsiasi altro telefono Avaya sprovvisto di licenza, in base all'ordine di registrazione.

Collegamenti correlati

Telefoni IP H.323 IP Office alla pagina 10
Riserva di licenze alla pagina 35

Riserva di licenze

Informazioni su questa attività

Non è possibile eseguire questa procedura finché non sarà stata creata la voce di interno. In caso di utilizzo della creazione automatica di interni (valore predefinito), la riserva della licenza non potrà essere effettuata se non successivamente all'installazione iniziale del telefono. È

tuttavia opportuno utilizzare con cautela questa impostazione con i telefoni esistenti già installati, per accertarsi che mantengano le licenze, se possibile, successivamente all'aggiunta di altri telefoni.

Generalmente, le licenze vengono assegnate automaticamente agli interni in ordine di registrazione. Tuttavia gli interni esistenti possono riservare una licenza in modo da assicurarsi che non sia andata persa quando i nuovi interni aggiunti al sistema vengono registrati per primi in seguito ad un riavvio di sistema.

- Sul sistema che utilizza le licenze WebLM, questa opzione è fissa, allo scopo di riservare una licenza.
- La riserva di licenze non è supportata nei sistemi in modalità Sottoscrizione.

Procedura

1. Tramite IP Office Manager, ricevere la configurazione dal sistema telefonico.
2. Selezionare **Interno** e quindi selezionare l'interno H.323.
3. Selezionate il tab **VoIP**.
4. Impostare il campo **Riserva licenza** su **Riserva licenza terminale Avaya IP**.
5. Ripetere il processo per ogni altro interno per cui si desidera riservare la licenza.
6. Salvare la configurazione.

Collegamenti correlati

Licenze e sottoscrizioni alla pagina 17

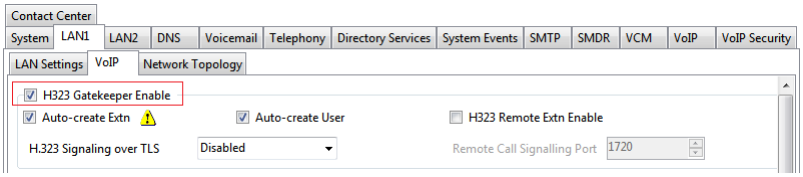
Capitolo 4: Abilitazione del gatekeeper H.323

Informazioni su questa attività

Il supporto per le linee e i telefoni H.323 è abilitato per impostazioni predefinite. È tuttavia necessario controllare le impostazioni.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.
4. Selezionare la sottoscheda **VoIP**.



5. Attivare la casella di controllo dell'impostazione **Attivazione gatekeeper H323**.
6. Salvare la configurazione.

Collegamenti correlati

Impostazione dell'intervallo di porte RTP alla pagina 37
Regolazione DiffServ QoS alla pagina 39
Codec predefiniti del sistema alla pagina 39

Impostazione dell'intervallo di porte RTP

Informazioni su questa attività

Le porte utilizzate per le chiamate VoIP H.323 variano per ciascuna chiamata. È possibile modificare l'intervallo per le porte utilizzate per evitare conflitti con altri servizi. Se il cliente dispone di firewall interni o di dispositivi simili che applicano filtri alla porta oppure inoltrano semplicemente il traffico in base alla porta utilizzata, l'intervallo impostato in questo campo deve essere autorizzato da tali dispositivi.

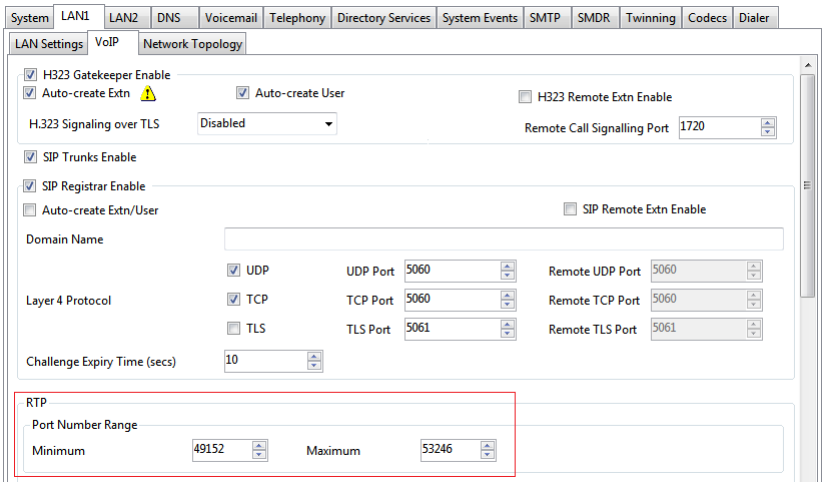
Per ogni chiamata VoIP, le porte di ricezione vengono selezionate dall'intervallo definito di seguito. I numeri pari nell'intervallo vengono utilizzati per il traffico di chiamate RTP (Real-Time

Transport Protocol) in entrata. Lo stesso traffico di chiamate RTCP (Real-Time Transport Control Protocol) utilizza il numero di porta RTP più 1, ossia numeri dispari.

È consigliabile utilizzare solo i numeri porta compresi tra 49152 e 65535, ossia quelli che rientrano nell'intervallo definito dalla IANA (Internet Assigned Numbers Authority) per l'uso dinamico.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.
4. Selezionare la sottoscheda **VoIP**.



5. Controllare la **Intervallo numeri porta** mostrata nella sezione **RTP**. Ricordare che il traffico RTCP corrispondente utilizza lo stesso intervallo più 1.
   - **Minima**: Impostazione predefinita = 49152. intervallo = da 1024 a 65280.

     Imposta il limite inferiore dei numeri di porta RTP utilizzati dal sistema. Scegliere un intervallo minimo inferiore a 1024 solo dopo aver esaminato attentamente l'intera configurazione.
   - **Massimo**: Impostazione predefinita = 53246. intervallo = da 1278 a 65534.

     Imposta il limite superiore dei numeri di porta RTP utilizzati dal sistema. Il divario tra intervallo minimo e massimo deve essere almeno 254. Scegliere un intervallo minimo inferiore a 1024 solo dopo aver esaminato attentamente l'intera configurazione.
6. Salvare la configurazione.

Collegamenti correlati

Abilitazione del gatekeeper H.323 alla pagina 37

Regolazione DiffServ QoS

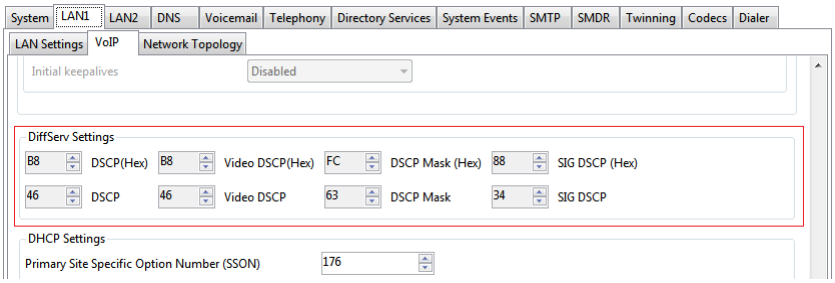
Informazioni su questa attività

DiffServ viene utilizzato per applicare diversi tag "QoS" (quality of service) agli elementi vocali (RTP) e al segnale di controllo (RTCP) di una chiamata VoIP. Il sistema IP Office non applica diverse priorità ai pacchetti di dati ricevuti o inviati in base ai relativi tag. Tuttavia, in caso di utilizzo in una rete che impiega QoS per la prioritizzazione da altri dispositivi, le impostazioni di IP Office devono essere impostate in modo da corrispondere a quelle previste per le chiamate vocali e i segnali di controllo

associati.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.
4. Selezionare la sottoscheda **VoIP**.



   Controllare che **Impostazioni DiffServ** vengano utilizzate dal sistema. Le due righe sono collegate: la riga superiore visualizza i valori DiffServ in numeri esadecimali, la riga inferiore visualizza i valori in numeri decimali. I valori esadecimali equivalgono ai decimali moltiplicati per 4. Ciascuna riga può essere utilizzata per impostare i valori richiesti.

5. Salvare la configurazione.

Collegamenti correlati

Abilitazione del gatekeeper H.323 alla pagina 37

Codec predefiniti del sistema

Informazioni su questa attività

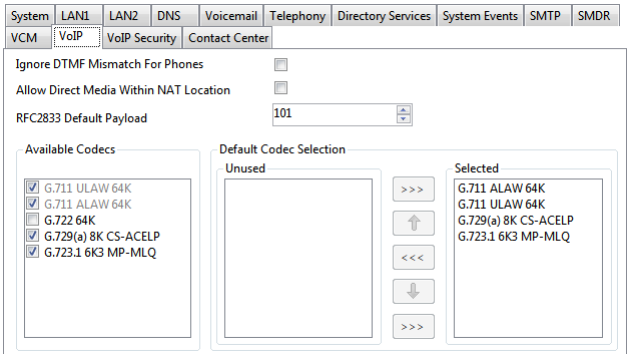
Per impostazione predefinita, tutti i dispositivi VoIP aggiunti alla configurazione di IP Office utilizzano le preferenze di codec predefiniti del sistema. Questa impostazione **Codec** viene visualizzata su un trunk IP o su un interno impostato su **Impostazioni predefinite del sistema**.

Oltre a poter modificare l'ordine delle preferenze dei codec predefiniti per tutti i trunk e gli interni VoIP, è possibile modificare le preferenze di codec utilizzate da un trunk o da un interno

specifico. Tuttavia, l'utilizzo delle impostazioni di sistema comuni garantiscono la coerenza dei codec tra trunk ed interni.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la sottoscheda **VoIP**.



La sezione relativa alla selezione predefinita consente di impostare l'ordine di preferenza dei codec predefiniti. Questo viene utilizzato da tutti gli interni (H.323 e SIP) e le linee IP nel sistema con l'impostazione **Selezione codec** impostata su **Impostazioni predefinite del sistema**. Si tratta del valore predefinito per tutti i nuovi interni e le nuove linee IP aggiunti.

L'elenco **Codec disponibili** mostra i codec supportati dal sistema. I codec abilitati in questo elenco possono essere utilizzati in altri tipi di configurazione, tra cui la selezione predefinita adiacente.

Avvertenza:

Se un codec presente in questo elenco viene deselezionato, sarà rimosso automaticamente da tutti gli elenchi di codec per linee e interni in cui era utilizzato.

4. Salvare la configurazione.

Collegamenti correlati

Abilitazione del gatekeeper H.323 alla pagina 37

Capitolo 5: Impostazioni DHCP

Per l'installazione di telefoni H.323 è consigliabile utilizzare DHCP, soprattutto in caso di installazione di un numero elevato di telefoni. Mediante DHCP è possibile semplificare i processi di installazione e manutenzione. Sono disponibili varie opzioni con cui scegliere il server da utilizzare per il supporto DHCP dei telefoni H.323:

- Se il sistema IP Office deve essere utilizzato come server DHCP per la rete, utilizzare la procedura descritta di seguito per controllare e configurare le impostazioni DHCP del sistema.
- Se dalla rete del cliente viene utilizzato un server DHCP separato, potrebbe essere necessario configurarlo per il supporto delle richieste DHCP da telefoni IP
- È possibile configurare IP Office affinché fornisca esclusivamente il supporto DHCP per telefoni Avaya. Questa opzione consente di utilizzarlo insieme a un altro server DHCP del cliente, senza dover configurare quest'ultimo per il supporto di telefoni IP.

Avvertenza:

- L'abilitazione di un server DHCP aggiuntivo in una rete può determinare problemi di collegamento per tutti i dispositivi nella rete. Verificare che l'utente e l'amministratore della rete concordino sulla scelta corretta dell'opzione server DHCP.

Collegamenti correlati

[Supporto DHCP del sistema](#) alla pagina 41
[Numeri opzione specifici per sito del sistema](#) alla pagina 42
[Modifica delle impostazioni SSON del sistema](#) alla pagina 42

Supporto DHCP del sistema

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.
4. Selezionare la scheda **Impostazioni LAN**
5. In **Numero di indirizzi IP assegnati tramite DHCP**, impostare il valore per il numero di indirizzi IP che il sistema può emettere.
6. In **Modalità DHCP**, selezionare **Server**.

7. Fare clic su **Avanzata**. Le impostazioni **Avanzata** consentono di regolare l'impostazione **DHCP**, inclusa l'aggiunta di più intervalli di numeri **DHCP** supportati dal sistema IP Office. Gli intervalli degli indirizzi all'esterno di quelli della subnet del sistema possono inoltre richiedere la creazione di instradamenti IP appropriati per garantire l'instradamento del traffico tra le subnet.

   Nota:

   - Non è necessario riavviare il sistema IP Office dopo aver modificato i pool DHCP. Tuttavia, i telefoni H323 Avaya e SIP connessi al sistema si riavvieranno. I telefoni IP non prodotti da Avaya non si riavviano, ma potrebbero richiedere un riavvio manuale per ottenere un indirizzo valido dalla nuova configurazione dei pool.

   Selezionare la casella di controllo **Applica solo al telefono IP Avaya**.

   IP Office agirà da server DHCP solo per i telefoni Avaya. Non è possibile utilizzare questa opzione se vengono supportati anche i telefoni della serie 1100 e 1200.

8. Salvare la configurazione.

Collegamenti correlati

Impostazioni DHCP alla pagina 41

Numeri opzione specifici per sito del sistema

In fase di richiesta delle impostazioni dell'indirizzo da un server DHCP, ogni telefono richiede inoltre ulteriori informazioni che il server DHCP potrebbe avere, inviando un numero di opzione specifico per sito (SSON, Site Specific Option Number). Se le informazioni nel server DHCP corrispondono al numero SSON, verranno incluse nella risposta DHCP.

I telefoni delle serie 1600 e 9600 utilizzano 242 come numero SSON predefinito. Mediante i menu del telefono è tuttavia possibile modificare il numero SSON utilizzato. Per i telefoni che utilizzano il sistema IP Office per DHCP, i numeri SSON supportati da IP Office vengono impostati nella configurazione del sistema IP Office. I valori utilizzati dai telefoni e supportati dal sistema IP Office devono corrispondere.

Collegamenti correlati

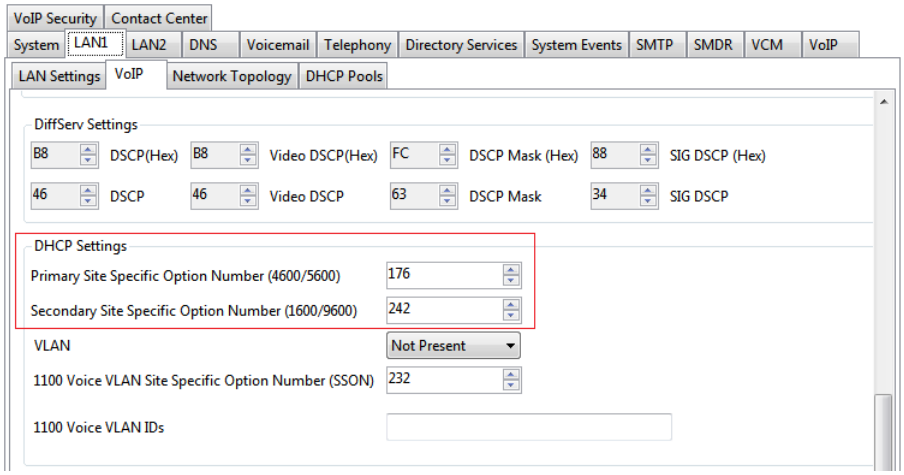
Impostazioni DHCP alla pagina 41

Modifica delle impostazioni SSON del sistema

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.

4. Selezionare la sottoscheda **VoIP**.



5. Verificare che le impostazioni per il numero opzione specifico per sito corrispondano a quelle richieste per il telefono supportato. Il numero predefinito per i telefoni delle serie 1600 e 9600 è 242.
6. Salvare la configurazione.

Collegamenti correlati

Impostazioni DHCP alla pagina 41

Capitolo 6: Impostazioni file server

Nell'ambito del processo di installazione, il telefono richiede i file da un file server. Usando DHCP, l'indirizzo del file server viene incluso nella risposta DHCP dal server DHCP. L'indirizzo del server dei file viene immesso nel telefono durante il processo di assegnazione degli indirizzi statici.

Di seguito sono indicate le opzioni del server dei file:

- Per i sistemi IP500 V2, è possibile utilizzare la scheda di memoria del sistema IP Office come origine per i file. Si tratta dell'opzione consigliata, valida per un massimo di 50 telefoni.
- Per i sistemi IP Office Server Edition è possibile utilizzare il disco del sistema come origine per i file utilizzati dai telefoni per la capacità completa del telefono supportata dal sistema.
- È possibile utilizzare il reindirizzamento HTTP per fare in modo che i file binari per i telefoni 9608, 9611, 9621 e 9641 vengano forniti da un server a parte, mentre il sistema IP Office fornisce tutti gli altri file.
- Anche l'applicazione IP Office Manager può agire da server dei file per un massimo di cinque telefoni. Se le opzioni qui sopra non sono accettabili o non corrispondono alle esigenze di capacità del sistema, è necessario un server dei file HTTP di terze parti. Nel server devono essere caricati i file del firmware del telefono necessari.

Utilizzo della porta

La porta utilizzata dai telefoni IP per richiedere file dipende dal tipo di telefono.

Porta	Utilizzo	Telefoni
80	Non protetto: Firmware, impostazioni e dati utente del telefono.	Tutte
411	Protetto: impostazioni, dati utente.	Telefoni H.323 9608, 9611, 9621 e 9641
443	Protetto: Firmware, impostazioni e dati utente del telefono.	Telefoni SIP
8411	Non protetto: firmware del telefono.	Telefoni remoti H.323

Per i telefoni più recenti, la porta da utilizzare può essere indicata tramite la risposta DHCP o il file di impostazioni fornito inizialmente al telefono. In assenza di risposta su tale porta, potrebbe essere eseguito il fallback del telefono su uno dei valori predefiniti della porta. Tuttavia, alcuni telefoni legacy più obsoleti sono codificati sulle porte fisse.

Collegamenti correlati

Modifica delle impostazioni del file server alla pagina 45
Impostazione del Server del File del Telefono alla pagina 46
Creazione/Modifica del File delle Impostazioni alla pagina 46
Modifica manuale del File alla pagina 48
Caricamento di file software nel sistema alla pagina 48

Modifica delle impostazioni del file server

Informazioni su questa attività

Se si utilizza il sistema IP Office per il supporto DHCP per i telefoni IP, sono disponibili varie opzioni nella configurazione del sistema IP Office per impostare gli indirizzi del file server inviati ai telefoni nelle risposte DHCP.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionate il tab **Sistema**.
4. Controllare l'impostazione **Tipo di server dei file del telefono**. Consultare Impostazione del Server del File del Telefono alla pagina 46.
5. In **Tipo di server dei file del telefono**, impostare le impostazioni in base alle esigenze. Vedere Impostazione del Server del File del Telefono alla pagina 46 per i dettagli sulle diverse impostazioni utilizzabili.
6. Per i telefoni 9608, 9611, 9621 e 9641, selezionare l'opzione **Reindirizzamento HTTP** per inviare le richieste per i file binari del telefono al separato **Indirizzo IP del server HTTP**.
7. Attivare la casella di controllo **Utilizza porte telefono preferite** per ridurre l'utilizzo delle porte HTTP/HTTPS configurate per la sicurezza del sistema (per impostazione predefinita, le porte 80 e 443) per le richieste dei file del telefono.
   - Quando la casella di controllo **Utilizza porte telefono preferite** è attivata, i file di impostazioni telefono generati automaticamente per i telefoni locali indicano la porta 8411 per HTTP e la 411 per TLS.
   - Quando la casella di controllo **Utilizza porte telefono preferite** è deselezionata, i file delle impostazioni telefono generati automaticamente e forniti dal sistema ai telefoni locali indicano le porte 80/411 o 80/443 in base al tipo di telefono.

     I file delle impostazioni telefono generati automaticamente e forniti dal sistema ai telefoni remoti indicano le porte 8411/411 o 8411/443 in base al tipo di telefono.
8. Abilitare la chekbox **Solo client HTTP Avaya** per fare in modo che il sistema risponda esclusivamente alle richieste dei file provenienti dai telefoni e dalle applicazioni Avaya.

   Nota:

   Non è opportuno utilizzare questa opzione se il sistema supporta anche i telefoni della serie 1100 e/o 1200.
9. Salvare la configurazione.

Collegamenti correlati

Impostazioni file server alla pagina 44

Impostazione del Server del File del Telefono

Le seguenti impostazioni vengono utilizzate per i telefoni H323 che richiedono file del firmware dal sistema IP Office:

Campo	Descrizione
Scheda di memoria (IP500 V2) **Disco** (IP Office Server Edition)	Utilizzare la memoria propria del sistema. L'indirizzo IP del sistema viene fornito come valori del server dei file TFTP e HTTP nella risposta DHCP. Questa è l'impostazione predefinita.
Manager	Utilizzare l'applicazione IP Office Manager come file server TFTP e HTTP. Questa opzione è supportata per un massimo di 5 telefoni IP. L'opzione utilizza l'indirizzo IP del PC Manager separato impostato nella configurazione. Il valore 0.0.0.0 predefinito viene utilizzato dal sistema per trasmettere eventuali applicazioni IP Office Manager disponibili in esecuzione nella rete. Si noti che, per impostazione predefinita, l'opzione IP Office Manager per il supporto TFTP è disabilitata (**File** > **Preferenze** > **Preferenze** > **Abilita server BootP e TFTP**).
Personalizzato	Questa opzione utilizza l'indirizzo IP del server TFTP separato e l'indirizzo IP del server HTTP impostati nella configurazione come indirizzi del file server nella risposta DHCP fornita ai telefoni.

Collegamenti correlati

Impostazioni file server alla pagina 44

Creazione/Modifica del File delle Impostazioni

Durante l'installazione, i telefoni richiedono in primo luogo il download di un file xxupgrade dal file server. Successivamente seguiranno le istruzioni contenute nel file per richiedere ulteriori file, se necessario. Per le varie serie di telefoni esistono file xxupgrade diversi. forniti con il firmware del telefono. Non modificare o cambiare in alcun modo i file xxupgrade.

L'ultima riga di tutti i file xxupgrade contiene indicazioni per richiedere il file `46xxsettings.txt`. Questo file consente di configurare specifiche impostazioni per tutti i telefoni IP H.323 Avaya supportati in un sito specifico.

Se si utilizza il sistema IP Office come file server, il sistema IP Office creerà automaticamente un file `46xxsettings.txt` appropriato in base a varie impostazioni di configurazione del sistema IP Office. Questa operazione si verificherà solo se nel server non è disponibile il file `46xxsettings.txt`.

Prefisso di composizione

Per i sistemi IP Office, l'aggiunta o la rimozione dei prefissi di composizione è compito del sistema IP Office invece che dei singoli telefoni. L'utilizzo delle regole di composizione avanzate tramite il file di impostazioni telefono non è supportato.

Supporto del protocollo 802.1Q

Se non è espressamente richiesto per la rete del cliente, è consigliabile modificare ## SET L2Q 0 in SET L2Q 2 per il funzionamento di IP Office.

Lingue telefoni serie 1600/9600

Oltre all'inglese, i telefoni delle serie 1600 e 9600 sono in grado di supportare fino ad altre 4 lingue. Questa operazione viene eseguita dai telefoni che effettuano il download dei file di lingua specificati nel file `46xxsettings.txt`. Attualmente vengono forniti 9 file di lingua non inglese nell'ambito dell'installazione di IP Office Manager.

Lingua	File 1600	File 9600
Olandese	mlf_dutch.txt	mlf_9600_dutch.txt
Francese (Canada)	mlf_french_can.txt	mlf_9600_french_can.txt
Francese	mlf_french_paris.txt	mlf_9600_french_paris.txt
Tedesco	mlf_german.txt	mlf_9600_german.txt
Italiano	mlf_italian.txt	mlf_9600_italian.txt
Portoghese	mlf_portuguese.txt	mlf_9600_portuguese.txt
Russo	mlf_russian.txt	mlf_9600_russian.txt
Spagnolo	mlf_spanish.txt	mlf_9600_spanish.txt
Spagnolo (America Latina)	mlf_spanish_latin.txt	mlf_9600_spanish_latin.txt

I file da scaricare sui telefoni sono definiti nelle sezioni `# SETTINGS1603`, `# SETTINGS1608` e `# SETTINGS1616` del file `46xxsettings.txt`. Per fare in modo che il telefono scarichi un file di lingua, rimuovere ## davanti a una delle opzioni `SET` e modificare il nome del file affinché corrisponda alla lingua desiderata. Se si utilizza il sistema IP Office come file server, è possibile fornire i file di lingua appropriati nella configurazione del sistema IP Office mediante la generazione automatica di file.

Backup/Ripristino

È possibile utilizzare un server HTTP come posizione in cui eseguire il backup e il ripristino delle impostazioni dei telefoni degli utenti quando i telefoni vengono connessi e disconnessi. Per i dettagli completi, vedere Impostazioni di backup e ripristino alla pagina 65.

Screensaver

È possibile specificare il numero di minuti che devono trascorrere prima che un telefono inattivo visualizzi un'immagine screen saver, nonché il nome del file di immagine. Consultare Screensaver alla pagina 63.

Collegamenti correlati

Impostazioni file server alla pagina 44

Modifica manuale del File

Procedura

1. Individuare il file `46xxsettings.txt` nel server dei file.
2. Utilizzando uno strumento di modifica del testo normale, aprire il file `46xxsettings.txt`.
3. Modificare il file come richiesto.

   Il file contiene numerosi commenti e note. Nel manuale dell'amministratore LAN Avaya appropriato sono disponibili ulteriori dettagli sulle varie impostazioni per ciascun tipo di telefono. Tenere presente che i file contengono inoltre un'ampia gamma di impostazioni utilizzate in altri sistemi telefonici Avaya che potrebbero non funzionare o essere supportate nei sistemi IP Office.

   Un carattere # all'inizio della riga è il comando sulla stessa riga.

Collegamenti correlati

Impostazioni file server alla pagina 44

Caricamento di file software nel sistema

Per i sistemi IP Office Server Edition, il firmware del telefono idoneo per il sistema IP Office è incluso nell'ambito dell'installazione del sistema IP Office nel server. In caso di utilizzo del sistema come file server per l'installazione del telefono non sono pertanto richiesti ulteriori interventi. Il firmware viene inoltre fornito come parte di IP Office Manager e copiato sul PC durante l'installazione di IP Office Manager. Non è possibile utilizzare altri firmware con IP Office, eccetto laddove documentato specificamente. Se necessario, è possibile controllare il firmware installato e copiare il nuovo firmware nel disco del sistema telefonico.

Il firmware del telefono idoneo per il sistema IP Office viene fornito con il software IP Office Manager e copiato nel PC quando IP Office Manager è installato. Non è possibile utilizzare altri firmware con IP Office, eccetto laddove documentato specificamente.

Esistono numerosi metodi in base ai quali è possibile copiare il firmware installato con IP Office nelle schede di memoria dei sistemi telefonici. Il metodo utilizzato dipende principalmente dal tipo di unità di controllo.

⚠ Avvertenza:

- Non rimuovere mai una scheda di memoria da un sistema in esecuzione senza arrestare prima la scheda o il sistema. Utilizzare IP Office Manager per arrestare la scheda di memoria prima che venga rimossa dal sistema.
- Per il funzionamento di IP Office, sulla scheda di memoria devono essere presenti solo i file del telefono con estensione bin. Altri file richiesti dai telefoni verranno generati automaticamente dal sistema in risposta a richieste da altri telefoni.

Collegamenti correlati

Impostazioni file server alla pagina 44

Unità di controllo IP500 V2

La scheda SD di sistema del sistema viene utilizzata per memorizzare i file. Si tratta di una scheda la cui presenza è obbligatoria in tutti i sistemi IP500 V2. I file del firmware vengono caricati nella scheda in diversi modi:

- Se il sistema è stato sottoposto a upgrade mediante l'opzione **Ricrea scheda SD** in IP Office Manager, il firmware verrà automaticamente copiato nella scheda durante il processo.
- Se è stata utilizzata la procedura guidata di upgrade di IP Office Manager, se è stata selezionata l'opzione **Carica file di sistema**, il firmware viene copiato sulla scheda come parte del processo. L'opzione **Carica file di sistema** è abilitata per impostazione predefinita.

Se si ritiene che non siano presenti i file corretti, è possibile utilizzare il File Manager integrato di IP Office Manager per verificare i file sulla scheda e copiarli su di essa, se necessario.

Collegamenti correlati

Impostazioni file server alla pagina 44

Utilizzo del Gestore File integrato per verificare e caricare i file

Informazioni su questa attività

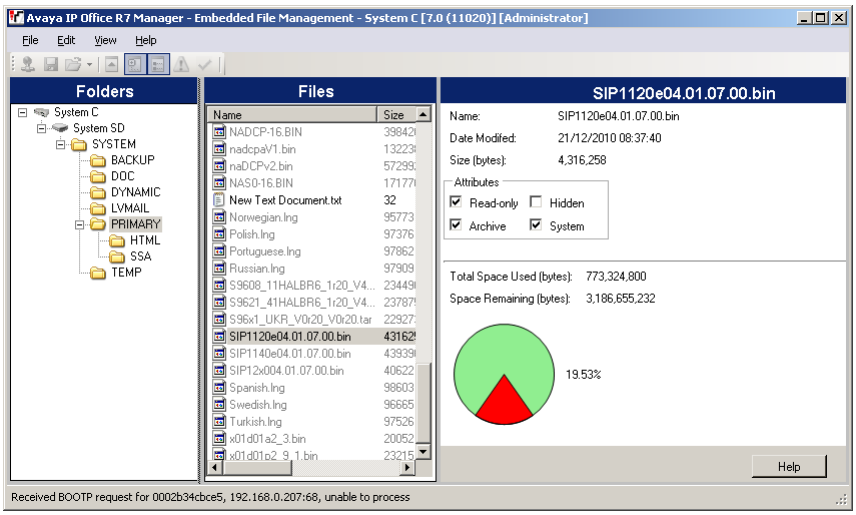
Il Gestore file integrato consente di visualizzare i file in remoto sulla scheda di memoria utilizzata dal sistema telefonico. Consente inoltre di caricare nuovi file.

Procedura

1. In IP Office Manager, selezionare **File** > **Avanzata** > **Gestione file incorporata**.

   Viene visualizzato il menu **Seleziona IP Office**.
2. Selezionare il sistema telefonico e fare clic su **OK**.
3. Inserire il nome e la password del sistema che corrispondono.

   Vengono visualizzati i contenuti della scheda di memoria.



4. Attenersi a una delle procedure seguenti:
   - Per IP500 V2 accedere a **SD di sistema** > **SISTEMA** > **PRIMARIO**.
   - Per IP Office Server Edition andare a **SISTEMA** > **PRIMARIO**
5. Per copiare i file, effettuare una delle operazioni seguenti:
   - Trascinare da **PRIMARIO** e rilasciare nella scheda di memoria.
   - Andare su **File** > **Carica file di sistema** > **Carica file telefoni** e selezionare il file da copiare.

   È possibile trovare i file sorgenti nel PC IP Office Manager in `C:\Program Files \Avaya\IPOffice\Manager\memory Cards\Common\system\primary`.

Collegamenti correlati

[Impostazioni file server](#) alla pagina 44

Copia manuale dei file

Informazioni su questa attività

È possibile copiare i file nella scheda di memoria posizionandoli in un PC con un alloggiamento specifico per schede di memoria.

Avvertenza:

- Non rimuovere mai una scheda di memoria da un sistema in esecuzione senza prima arrestarlo utilizzando la procedura seguente.

Procedura

1. Tramite IP Office Manager, selezionare **File** > **Avanzata** > **Comando scheda di memoria** > **Arresto**.

   Viene visualizzato il menu **Seleziona IP Office**.
2. Selezionare il sistema telefonico e fare clic su **OK**.
3. Inserire il nome e la password del sistema che corrispondono.

4. È possibile che venga richiesto di scegliere la scheda da arrestare. Selezionare **Sistema** e fare clic su **OK**.
5. Sul retro dell'unità di controllo, verificare che i LED dello slot della scheda di memoria siano spenti prima di rimuovere la scheda.
6. Posizionare la scheda nello slot delle schede di memoria del PC e analizzarne i contenuti.
7. Nel sistema IP500 V2, andare a **SD di sistema** > **SISTEMA** > **PRIMARIO**.

   È possibile trovare i file di origine nel PC IP Office Manager in `C:\Program Files\Avaya\IP Office\Manager\memory Cards\Common\system\primary`.

Risultato

In caso di reinserimento della scheda nel sistema, l'utilizzo della stessa viene automaticamente riavviato.

Collegamenti correlati

Impostazioni file server alla pagina 44

Caricamento di file in un Server di terze Parti

I file del firmware del telefono vengono installati nell'ambito dell'applicazione IP Office Manager e si trovano nella directory di installazione dell'applicazione. Per impostazione predefinita, la directory si trova al percorso `c:\Program Files\Avaya\IP Office\Manager`.

Gli stessi file firmware possono essere ottenuti direttamente dal pacchetto software utilizzato per installare IP Office Manager senza dover eseguire l'installazione. I file si trovano nella sottocartella `\program files\Avaya\IPOffice\Manager` della directory di installazione.

Questi set includono file con estensione bin utilizzati anche per altri dispositivi, incluso il sistema IP Office stesso.

Collegamenti correlati

Impostazioni file server alla pagina 44

Capitolo 7: Creazione di utenti e interni

Se un nuovo telefono H.323 effettua la registrazione al sistema, quest'ultimo può creare automaticamente una nuova voce interno per il telefono nella configurazione. nonché una nuova voce utente per il telefono. In alternativa, se il telefono effettua la registrazione mediante un numero di interno per cui esiste già una voce, verrà considerata questa voce a condizione che non sia già utilizzata da altri telefoni.

Per le nuove installazioni, l'opzione Creazione automatica può essere utilizzata per semplificare l'aggiunta di più telefoni. Successivamente all'installazione, è necessario disabilitare le opzioni di creazione automatica. Se non viene utilizzata la creazione automatica, sarà necessario aggiungere automaticamente alla configurazione le voci di interni e utenti prima di tentare l'installazione dei telefoni.

Collegamenti correlati

Password interno predefinita alla pagina 52
Creazione manuale Utenti alla pagina 53
Creazione manuale dei numeri di interno alla pagina 53
Selezione del codec richiesto alla pagina 54
Utilizzo della creazione automatica alla pagina 55

Password interno predefinita

Informazioni su questa attività

La registrazione della maggior parte dei telefoni SIP richiede l'immissione di una password. Questa impostazione può essere impostata tramite l'impostazione **Password predefinita interno** del sistema. In alternativa, è possibile impostare una password specifica per un determinato interno tramite le impostazioni dell'interno.

Le impostazioni dell'interno creato automaticamente in un sistema non possono essere abilitate fino a che non si configura questo valore. Verrà quindi utilizzata come password per qualsiasi interno creato automaticamente.

Procedura

1. Utilizzando IP Office Manager o IP Office Web Manager in modalità offline, caricare la configurazione del sistema.
2. Selezionare **Sistema** o **Impostazioni di sistema** > **Sistema**.
3. Selezionare **VoIP**.
4. Selezionare **Sicurezza VoIP**.

5. Nella sezione **Password predefinita interno**:
   a. Fare clic sull'icona per visualizzare/nascondere la password corrente.
   b. Se necessario, modificare o rimuovere la password.

      La password può essere vuota o può contenere dalle 9 alle 13 cifre (0-9).
6. Salvare le impostazioni.

Collegamenti correlati

Creazione di utenti e interni alla pagina 52

Creazione manuale Utenti

Informazioni su questa attività

Se l'opzione Creazione automatica utente non è abilitata, è necessario creare manualmente una voce utente per ogni telefono installato. Per creare manualmente una voce, attenersi alla procedura descritta di seguito. Verrà inoltre richiesto se è necessario creare una voce di interno corrispondente.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Per visualizzare l'elenco degli utenti esistenti, fare clic su **Utente**
3. Fare clic con il pulsante destro del mouse sul riquadro di destra e selezionare **Nuovo**.
   a. Nella scheda **Utente** impostare quanto segue:
      - **Nome**: Immettere un nome per l'utente dell'interno. Il nome deve essere univoco. Se Voicemail è in funzione, il nome viene utilizzato come base per una nuova casella di posta con nome corrispondente.
      - **Interno**: Questo deve corrispondere al numero di interno.
   b. Fare clic su **OK**.

      IP Office Manager richiede di creare un interno corrispondente.
   c. Selezionare **Interno H.323** e immettere la password del telefono per l'interno. Fare clic su **OK**.
4. Salvare la configurazione.

Collegamenti correlati

Creazione di utenti e interni alla pagina 52

Creazione manuale dei numeri di interno

Informazioni su questa attività

Se l'opzione Creazione automatica interno non è abilitata, è necessario creare manualmente una voce di interno per ogni telefono installato. È possibile eseguire queste operazioni

contestualmente al processo di creazione manuale di utenti oppure separatamente, mediante la procedura indicata di seguito.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Per visualizzare l'elenco degli interni esistenti, fare clic su **Interno**
3. Fare clic su **Nuovo**.
4. Nella scheda **Int**, impostare quanto segue:
   a. **ID interno**: Per gli interni VoIP, immettere un numero sufficientemente lungo da risultare univoco, ovvero non utilizzato da un altro interno.
   b. **Interno di base**; Immettere il numero di interno che si intende assegnare al telefono. Anche in questo caso il numero deve essere univoco. Questo valore è associato all'interno con l'utente provvisto dello stesso numero.
   c. **Password telefonica**: Questa è la password utilizzata per registrare il telefono nel sistema. Se non è stata impostata, viene utilizzata quella dell'utente corrispondente **Codice accesso**.
5. Per aggiungere il nuovo numero di interno, fare clic su **OK**.
6. Salvare la configurazione.

Collegamenti correlati

Creazione di utenti e interni alla pagina 52

Selezione del codec richiesto

Informazioni su questa attività

Se **Selezione codec** è impostato su **Impostazioni predefinite del sistema**, l'interno utilizza le preferenze codec del sistema . Nella maggior parte dei casi è preferibile mantenere l'impostazione predefinita. Qualsiasi modifica necessaria deve essere apportata a livello di sistema, per garantire la coerenza di tutti gli interni e i trunk IP.

Se necessario, è tuttavia possibile regolare il valore **Selezione codec** di ogni singolo trunk e interno, affinché differisca dai valori di sistema predefiniti.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Per visualizzare le impostazioni dell'interno, fare clic su **Interno**.
3. Selezionate il tab **VoIP**.
4. Modificare **Selezione codec** a **Personalizzato**.

   È possibile utilizzare gli elenchi **Non in uso** e **Selezionato** per selezionare i codec utilizzati dal dispositivo e il relativo ordine di preferenza.
5. Salvare la configurazione.

Collegamenti correlati

Creazione di utenti e interni alla pagina 52

Utilizzo della creazione automatica

Informazioni su questa attività

Se viene installato un numero elevato di telefoni, esclusi i casi in cui la configurazione è stata preimpostata, la creazione automatica consente di semplificare il processo di installazione. Agli utenti creati automaticamente vengono assegnate le impostazioni dei diritti utente Creazione automatica IP. Per impostazione predefinita, le chiamate in uscita non sono consentite per questo set di diritti utente.

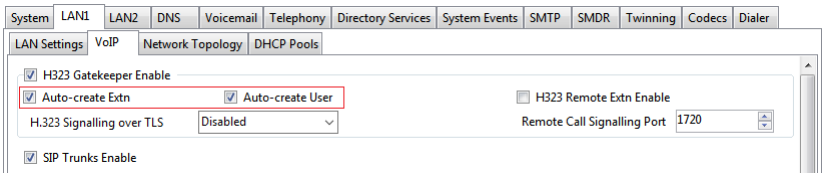
- Disabilitazione automatica della creazione automatica: È caldamente sconsigliato lasciare abilitate le impostazioni per la creazione automatica di interni e utenti. Per la versione 9.1 e successive, il sistema disabilita automaticamente l'impostazione 24 ore dopo l'abilitazione.
- Non supportato con la gestione licenze WebLM: Le opzioni di utenti e interni a creazione automatica non sono utilizzabili nei sistemi configurati per acquisire licenze da un servizio WebLM.

Prerequisiti

Nella versione 11.0.4.0 e successive, è necessario impostare la password dell'interno predefinito prima di abilitare la creazione automatica.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.
4. Selezionare la sottoscheda **VoIP**.



5. Configurare le impostazioni **Creazione automatica interno** e **Creazione automatica utente**

   Nota:

   È necessario creare manualmente le voci di interno e/o le voci utente prima di installare i telefoni.

   Nei sistemi precedenti alla versione 11.0.4.0, impostare e confermare una password, quando viene selezionato **Creazione automatica interno**. La password viene impostata come Password Telefono per tutti gli interni creati automaticamente. La password del telefono viene utilizzata per la registrazione.

6. Salvare la configurazione.

Collegamenti correlati

Creazione di utenti e interni alla pagina 52

Capitolo 8: Collegamento del telefono

Informazioni su questa attività

In questa procedura il telefono viene collegato alla fonte di alimentazione e alla LAN Ethernet. Non appena il telefono è alimentato inizierà a richiedere informazioni.

Prerequisiti

Assicurarsi di aver completato l'installazione del telefono prima di iniziare a connetterlo.

Procedura

1. Collegare un cavo di rete LAN alla presa di entrata dei dati dell'alimentatore utilizzato dal telefono.
2. Collegare il cavo LAN in dotazione con il telefono IP dalla presa di dati e alimentazione in uscita alla presa con la porta LAN  situata sulla parte posteriore del telefono IP.

   L'indicatore dei messaggi del telefono si illumina di rosso per alcuni secondi. Il telefono avvia il processo di caricamento del software. Dopo un breve periodo, il telefono visualizzerà `Inizializzazione`, quindi `Caricamento`. La fase di caricamento può durare alcuni minuti.

   - Se sul telefono è presente un file di avvio software (ovvero se è stato installato in precedenza), il telefono carica il file e visualizzerà `Avvio in corso`.
3. Se il telefono visualizza `No Ethernet`, verificare il collegamento alla LAN.

   Il telefono visualizza `DHCP` e un timer mentre tenta di richedere un indirizzo IP e altre informazioni a un server DHCP.
4. Premere * mentre `DHCP` viene visualizzato per passare all'installazione dell'indirizzo statico. Vedere installazione dell'indirizzo statico.

   Dopo alcuni secondi, la negoziazione DHCP viene completata. Se il timer supera i 60 secondi, indica un errore di funzionamento della rete o di configurazione del server DHCP.

   Una volta completata la richiesta DHCP, il telefono richiederà i file dal file server indicato nella risposta DHCP. Il primo file richiesto contiene i dettagli degli altri file che devono essere caricati dal telefono. Il telefono effettua la richiesta dei file mediante HTTPS. In caso di esito negativo, effettua la stessa richiesta mediante HTTP. In caso di esito negativo, effettua una richiesta finale mediante TFTP. Se tutte le richieste avranno esito negativo, il telefono utilizza la versione corrente del file presente nella memoria.

   Il telefono avvia un ciclo di richiesta, caricamento e quindi trasferimento di file nella propria memoria flash.

   Dopo aver caricato i file, il telefono visualizza `Int. =`. consultare Registrazione del telefono alla pagina 57.

Collegamenti correlati

Registrazione del telefono alla pagina 57
Elenco dei telefoni registrati alla pagina 57

Registrazione del telefono

Informazioni su questa attività

Per i nuovi telefoni e i telefoni che sono stati reimpostati, il telefono richiede un numero di interno.

- Se la creazione automatica è abilitata, il numero di interno utilizzato, se disponibile, crea un nuovo interno e nuove voci utente nella configurazione di IP Office.
- Se la creazione automatica non è abilitata, il numero di interno utilizzato deve corrispondere a una voce di interno VoIP nella configurazione di IP Office, consultare Creazione manuale dei numeri di interno alla pagina 53.

Procedura

1. In **Int** immettere il numero di interno che il telefono deve utilizzare e premere #.

   Nota:

   Il telefono visualizza `Tipo apparecchio errato` se si tenta di utilizzare il numero di un interno non-IP esistente.

2. In **Password**, effettuare una delle seguenti operazioni:
   - Se si utilizza la creazione automatica per un interno, immettere la password specificata durante l'attivazione della creazione automatica.
   - Se non si utilizza la creazione automatica, immettere la **Password telefonica** come impostato nella configurazione del sistema per l'interno. Se non è stato impostata una **Password telefonica**, il sistema effettua il controllo rispetto all'utente corrispondente **Codice accesso**.

   Nota:

   Il sistema disabilita l'utilizzo delle password predefinite, come 0000, supportate da alcuni telefoni. Consultare Blocco dei passcode predefiniti alla pagina 28.

3. Verificare che, con quell'interno, sia possibile effettuare e ricevere chiamate.

Collegamenti correlati

Collegamento del telefono alla pagina 56

Elenco dei telefoni registrati

Informazioni su questa attività

È possibile utilizzare l'applicazione Monitoraggio del Sistema per controllare quali telefoni hanno effettuato la registrazione al sistema.

Procedura

1. Avviare Monitoraggio del Sistema e connettersi al sistema IP Office.
2. Selezionare **Stato** > **Stato telefono H.323**.

Risultato

Il Monitoraggio di Sistema visualizza i telefoni registrati e quanti sono attualmente in attesa di registrazione. È necessario selezionare l'opzione di filtro **Sistema** > **Stampa traccia** per visualizzare questi messaggi.

Gli elementi indicati di seguito appaiono sotto forma di righe del modulo:

```
792 ms PRN: GRQ da c0a82c15 --- RAS raggiunge la capacità massima di
10; Terminali registrati 41
```

Collegamenti correlati

Collegamento del telefono alla pagina 56

Parte 3: Configurazione opzionale

Capitolo 9: Abilitazione del monitoraggio della qualità RTCP

I telefoni IP Avaya supportano il monitoraggio della qualità delle chiamate. L'abilitazione del monitoraggio RTCP fornisce al sistema misure sul ritardo dei pacchetti, sulla perdita dei pacchetti e sul jitter. È possibile accedere a tali informazioni utilizzando le applicazioni System Status e System Monitor. È inoltre possibile configurare allarmi di sistema per segnalare i casi in cui i valori di qualità delle chiamate superano i livelli impostati.

È possibile inviare i rapporti sulla qualità delle chiamate RTCP anche all'indirizzo di un'applicazione di monitoraggio QoS di terzi.

Per la versione IP Office 10.0 e successive, oltre ai telefoni singoli, anche il sistema può inviare i rapporti RTCP sulla qualità delle chiamate.

Collegamenti correlati

Abilitazione dei rapporti sulla qualità del telefono alla pagina 60
Abilitazione dei rapporti sulla qualità del sistema alla pagina 61
Impostazione dei Livelli di Allarme per la Qualità alla pagina 62

Abilitazione dei rapporti sulla qualità del telefono

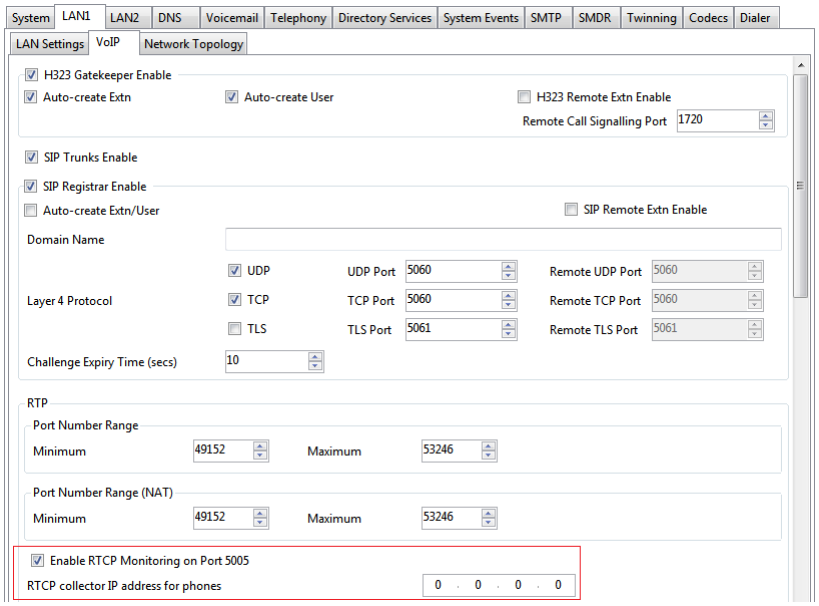
Informazioni su questa attività

I rapporti sulla qualità delle chiamate RTCP dai telefoni vengono abilitati a livello centrale, attraverso le impostazioni del sistema.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2** a seconda di quale interfaccia LAN del sistema si desidera utilizzare per supportare gli interni H.323.

4. Selezionare la sottoscheda **VoIP**.



5. Attivare la casella di controllo **Abilita monitoraggio RTCP su porta 5005**.

   Per impostazione predefinita, i dati RTCP vengono inviati al sistema IP Office. immettere l'indirizzo nel campo **Indirizzo IP raccolta RTCP per i telefoni** per i telefoni inviare i dati a un indirizzo specifico per l'acquisizione da parte di un'applicazione di monitoraggio QoS di terze parti.

6. Salvare la configurazione.

Collegamenti correlati

[Abilitazione del monitoraggio della qualità RTCP](#) alla pagina 60

Abilitazione dei rapporti sulla qualità del sistema

Informazioni su questa attività

Per la versione IP Office 10.0 e successive, oltre ai telefoni singoli, anche il sistema può inviare i rapporti RTCP sulla qualità delle chiamate.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **Telefonia**, quindi la sottoscheda **Telefonia**.
4. Andare alla sezione **Configurazione del modulo di raccolta RTCP**.
   a. Abilitare la casella di controllo **Invia RTCP a una raccolta RTCP**.
   b. In **Indirizzo server** aggiungere l'indirizzo dell'applicazione di monitoraggio QoS di terze parti alla quale il sistema invia i rapporti RTCP.

c. In **Numero porta UDP** immettere la porta di destinazione. L'impostazione predefinita è 5005.

d. In **Intervallo rapporti RTCP** immettere la frequenza dell'invio di rapporti RTCP da parte del sistema.

5. Salvare la configurazione.

Collegamenti correlati

Abilitazione del monitoraggio della qualità RTCP alla pagina 60

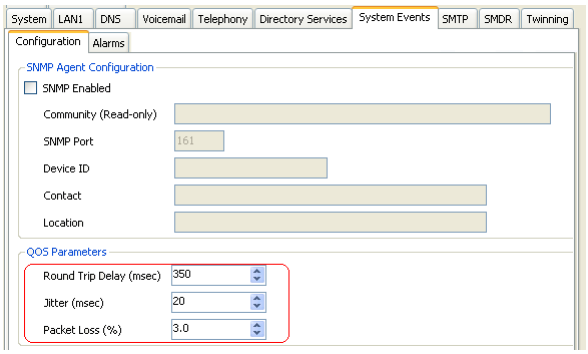
Impostazione dei Livelli di Allarme per la Qualità

Informazioni su questa attività

Il sistema può inviare allarmi di qualità della chiamata all'applicazione System Status. Può inviare gli stessi allarmi anche a SNMP, e-mail o destinazioni Syslog. Per ulteriori informazioni su come configurarli, consultare la documentazione di IP Office Manager. Le impostazioni indicate di seguito consentono di impostare i livelli che, se superati, determinano l'invio di un allarme al termine di una chiamata.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Selezionare **Sistema**.
3. Selezionare la scheda **Eventi di sistema**, quindi la sottoscheda **Configurazione**.



I parametri QoS vengono utilizzati dal sistema per attivare allarmi. Le impostazioni predefinite corrispondono ai limiti generalmente accettabili per una qualità soddisfacente delle chiamate

4. Salvare la configurazione.

Collegamenti correlati

Abilitazione del monitoraggio della qualità RTCP alla pagina 60

Capitolo 10: Screensaver

Dopo un determinato tempo di inattività, i telefoni della serie 9600 possono visualizzare un'immagine screen saver. Finché il telefono resta inattivo, l'immagine si sposta in una posizione casuale dello schermo ogni 5 secondi.

Per i telefoni completamente supportati dal sistema IP Office, viene fornito automaticamente un file predefinito dal sistema IP Office. In caso contrario:

- Il timeout per lo screen saver e il nome del file di immagine vengono impostati mediante la personalizzazione del file `46xxsettings.txt`.
- Il file di immagine da utilizzare deve essere caricato nel server dei file utilizzato dai telefoni.

Di seguito sono riportati i requisiti dell'immagine

- Formato: immagini JPG.
- Dimensioni massime Pixel: Le dimensioni dell'immagine devono essere minori di quelle dello schermo del telefono. Se l'immagine è più grande, non verrà visualizzata. Se sono presenti vari tipi di telefono che utilizzano la stessa immagine, questa deve essere più piccola rispetto alla dimensione massima di tutti i tipi di telefono. Se si utilizza il file 46xxsettings.txt per specificare le impostazioni dello screen saver, è possibile indicare un'immagine separata per ciascun tipo di telefono.

Telefono	Dimensioni massime
9611	160x160
9621G	320x160
9614G	320x240

- Display a colori: la profondità del colore è di 16 bit. Un'immagine a colori separata avrà una resa migliore.
- Display in bianco e nero: Un logo in un'unica scala di grigio avrà una resa migliore. Sono supportati 2 livelli di scala di grigio.
- Trasparenza: Per richiamare uno sfondo trasparente, utilizzare un colore di sfondo di 0,255,0 (il verde più brillante).

Le impostazioni predefinite di IP Office prevedono l'utilizzo di un file di immagine denominato 96xxiposs.jpg. Mediante il gestore file integrato in IP Office Manager, sostituire il file presente nella cartella /primary del sistema con l'immagine personalizzata. Riavviare i telefoni per consentire il caricamento della nuova immagine.

Collegamenti correlati

Personalizzazione delle impostazioni dello screensaver alla pagina 64

Personalizzazione delle impostazioni dello screensaver

Informazioni su questa attività

Il funzionamento predefinito prevede l'utilizzo dell'immagine singola `96xxiposs.jpg`, sostituibile con una personalizzata. Se si utilizza un file `46xxsettings.txt` personalizzato, è possibile impostare timeout di inattività per la visualizzazione dello screen saver e il nome dell'immagine.

Procedura

1. Creare un file JPG per il cliente che soddisfi i requisiti.

   In questo esempio viene utilizzato il nome del file `logo.jpg`.

2. Scaricare il file `46xxsettings.txt` corrente dal server dei file utilizzato dai telefoni.
3. Aggiungere le righe seguenti al file `46xxsettings.txt`:

   ```
   ## SET SCREENSAVER nome file
   SET SCREENSAVER logo.jpg
   ## SET SCREENSAVERON tempo in minuti prima dell'attivazione
   SET SCREENSAVERON 40
   ```

   - Utilizzo di immagini separate per ciascun tipo di telefono

     L'aggiunta di quanto sopra all'inizio del file si riflette su tutti i tipi di telefono. Aggiungendo impostazioni diverse per ciascuna delle varie sezioni MODEL4 del file per i vari tipi di telefono è possibile utilizzare immagini separate per ciascun tipo di telefono.

4. Caricare i nuovi file nel server dei file utilizzato dai telefoni.
5. Riavviare i telefoni per consentire il caricamento della nuova immagine e delle nuove impostazioni.

Collegamenti correlati

Screensaver alla pagina 63

Capitolo 11: Impostazioni di backup e ripristino

I telefoni IP H.323 serie 1600 e 9600 supportano il backup e il ripristino dei dati specifici degli utenti su server HTTP. L'indirizzo per questo server di backup viene impostato separatamente rispetto a quello del file server utilizzato per il firmware del telefono.

Queste opzioni vengono utilizzate se il percorso del server HTTP per il backup e il ripristino è stato specificato nel file `46xxsettings.txt` del telefono.

- L'indirizzo del server HTTP utilizzato per le operazioni di backup/ripristino è separato dall'indirizzo del server HTTP utilizzato per il download dei file firmware dei telefoni.
- Per consentire ai telefoni di inviare file al server HTTP è necessario apportare alcune modifiche alla configurazione del server utilizzato per il backup/ripristino.
- Se il sistema IP Office viene utilizzato come file server per l'installazione del telefono, può inoltre essere utilizzato per le funzioni di backup e ripristino, compresa la generazione automatica del file. Quando si utilizza la generazione automatica, alcune impostazioni del file di ripristino sono basate sulle impostazioni IP Office dell'utente. Si tratta quindi della soluzione consigliata, laddove possibile.

Il backup viene utilizzato quando l'utente del telefono si disconnette dal telefono. Durante la procedura di disconnessione, il telefono genera un file contenente i dati dell'utente e lo invia alla posizione BRURI. Il nome del file è composto dal numero di interno dell'utente seguito da `_16xxdata.txt`, ad esempio `299_16xxdata.txt`.

Il ripristino viene utilizzato quando l'utente si collega al telefono. Il telefono invia la richiesta del file appropriato in base al numero di interno dell'utente. Se il file viene recuperato correttamente, il telefono importerà le impostazioni, visualizzerà il messaggio `Recupero riuscito` e continuerà a funzionare normalmente. Se il file non può essere recuperato, verrà visualizzato il messaggio `Recupero non riuscito` e il telefono continuerà a utilizzare le impostazioni esistenti.

Collegamenti correlati

Come specificare il valore BRURI alla pagina 66
Autenticazione HTTP alla pagina 66
Controllo Manuale dei Backup/Ripristini alla pagina 67
File di esempio alla pagina 67

Come specificare il valore BRURI

Informazioni su questa attività

Se si utilizza il sistema IP Office come server dei file, è consigliabile utilizzarlo anche come server di backup e ripristino. Questa opzione non richiede configurazioni aggiuntive. Se il file `46xxsettings.txt` non è presente nel sistema IP Office, verrà generato automaticamente quando richiesto da un telefono e includerà il proprio indirizzo IP come indirizzo del server di backup e ripristino. Se il file `46xxsettings.txt` è presente nel sistema IP Office, è possibile modificare manualmente l'indirizzo del server di backup e ripristino mediante il processo indicato di seguito affinché corrisponda all'indirizzo IP del sistema.

Se si desidera utilizzare un altro server, modificare il valore `BRURI` nel file `46xxsettings.txt`. Sarà inoltre necessario verificare che il server utilizzato sia configurato per consentire il caricamento dei file nella cartella specificata del server.

Procedura

1. Aprire il file `46xxsettings.txt`.
2. Individuare la riga contenente il valore **IMPOSTA BRURI**.
3. Se la riga è preceduta da caratteri #, rimuovere tali caratteri e gli eventuali spazi presenti.
4. Dopo `SET BRURI`, inserire uno spazio e quindi l'indirizzo del server HTTP di backup:
   - Ad esempio `SET BRURI http://192.168.0.28`
   - Se necessario, specificare il percorso a una directory specifica del server e/o includere un numero di porta specifico, ad esempio: `SET BRURI http://192.168.0.28/backups:8080`.

Collegamenti correlati

Impostazioni di backup e ripristino alla pagina 65

Autenticazione HTTP

È supportata l'autenticazione HTTP. Se impostata, verrà utilizzata sia per le operazioni di backup che di di ripristino. Le credenziali e l'area di autenticazione sono archiviate nella memoria riprogrammabile non volatile del telefono, che non viene sovrascritta quando si scarica il nuovo firmware.

I valori predefiniti delle credenziali e dell'area di autenticazione sono Null. Se il server HTTP richiede l'autenticazione, viene richiesto all'utente di inserire le nuove credenziali tramite il telefono. Se l'autenticazione ha esito positivo, i valori utilizzati vengono archiviati e utilizzati per le successive operazioni di backup e ripristino.

Collegamenti correlati

Impostazioni di backup e ripristino alla pagina 65

Controllo Manuale dei Backup/Ripristini

Gli utenti possono richiedere un backup o ripristino tramite la schermata Opzioni di Backup/ Ripristino **Avanzata**, come descritto nella guida per l'utente del modello di telefono specifico.

Collegamenti correlati

[Impostazioni di backup e ripristino](#) alla pagina 65

File di esempio

Di seguito viene riportato un esempio di un file di backup/ripristino dei dati utente di un telefono di serie 1600. I valori vengono trascritti solo nel caso in cui siano stati modificati rispetto all'impostazione predefinita.

Se le operazioni di backup e ripristino vengono effettuate mediante la generazione automatica dei file, gli elementi contrassegnati da * verranno controllati dai valori archiviati e forniti dalle impostazioni IP Office dell'utente.

File	Campi	Descrizione
ABKNAME001=Int201 ABKNUMBER001=201 ABKNAME002=Int201ad ABKNUMBER002=201 ABKNAME003=Int203 ABKNUMBER003=203 Redial=0 Call Timer=0 Visual Alerting=1 Call Log Active=1 Log Bridged Calls=1 Log Line Calls=1 Log Calls Answered by Others=0 Audio Path=2 Personalized Ring=7 Handset AGC=1 Headset AGC=1 Speaker AGC=1 Error Tone=1 Button Clicks=0 Display Language=English	ABKNAMEmmm ABKNUMBERmmm	Queste voci accoppiate sono utilizzate per i contatti personali inseriti nel telefono. Il valore mmm in ogni coppia di voci viene sostituito da un numero di 3 cifre a partire da 001. La prima riga della coppia archivia il nome del contatto, la seconda riga archivia il numero di telefono del contatto.*
	LANGUSER	Indica la lingua visualizzata. Il nome della lingua viene archiviato.*
	LOGACTIVE	Registro chiamate attivato su (1) o disattivato (0).*
	LOGBRIDGED	Registro chiamate in parallelo attivato (1) o disattivato (0).*
	LOGLINEAPPS	Registro chiamate su linea attivato (1) o disattivato (0).*
	LOGOTHERANS	Registro chiamate a cui hanno risposto altri attivato (1) o disattivato (0).*
	OPTAGCHAND	Controllo automatico del guadagno dell'apparecchio attivato (1) o disattivato (0).

La tabella continua…

File	Campi	Descrizione
	OPTAGCHEAD	Controllo automatico del guadagno delle cuffie attivato (1) o disattivato (0).
	OPTAGCSPKR	Controllo automatico del guadagno dell'altoparlante attivato (1) o disattivato (0).
	OPTAUDIOPATH	Percorso Audio.*
	OPTCLICKS	Clic tasti attivato (1) o disattivato (0).*
	OPTERRORTONE	Tono di errore attivato (1) o disattivato (0).*
	PERSONALRING	Suoneria personalizzata. Viene archiviato un valore numerico (da 1 a 8) per la suoneria selezionata.*
	PHNREDIAL	Ricomposizione
	PHNSCRONCALL	Passaggio alla schermata della chiamata, con chiamata attivata (1) o disattivata (0).
	PHNSCRONALERT	Passaggio alla schermata di chiamata con squillo attivato (1) o disattivato (0).
	PHNTIMERS	Timer chiamate attivato (1) o disattivato (0). ✓
	PHNVISUALALERT	Avvisi visivi attivati (1) o disattivati (0). ✓

Collegamenti correlati

[Impostazioni di backup e ripristino](#) alla pagina 65
[Configurazione del server IIS](#) alla pagina 68
[Configurazione del server apache](#) alla pagina 69

Configurazione del server IIS

Informazioni su questa attività

Creare una cartella di backup al di sotto della directory principale del server Web. Tutti i file di backup verranno archiviati in questa directory. Ad esempio, se la tua cartella di backup è `C:/Inetpub/wwwroot/backup`, il file `46xxsettings.txt` deve avere una linea simile a `SET BRURI http://www.example.com/backup`.

Procedura

1. Andare su **Avvia** > **Impostazioni** > **Pannello di controllo** > **Strumenti di amministrazione** e selezionare , a seconda della versione di Windows, **Manager di Internet Information Services** o **Servizi di informazioni su Internet**.
2. Fare clic con il pulsante destro del mouse sulla cartella creata per il backup. Fare clic con il pulsante destro del mouse su **Sito Web predefinito** se non è presente una directory specifica per il backup.
3. Selezionare **Proprietà**.
4. Nella scheda **Rubrica**, attivare la casella di controllo **Formato**.
5. Attenersi alla procedura seguente per configurare IIS 6.0:
   a. Accedere a **Avvia** > **Impostazioni** > **Pannello di controllo** > **Strumenti di amministrazione**.
   b. Sotto **Sito Web predefinito**, selezionare **Estensione dei servizi Web**
   c. Verificare che l'opzione **WebDAV** sia impostata su **Consentito**.

Collegamenti correlati

File di esempio alla pagina 67

Configurazione del server apache

Informazioni su questa attività

Creare una cartella di backup al di sotto della directory principale del server Web. Concedere a tutti l'accesso in scrittura. Tutti i file di backup verranno archiviati in questa directory. Ad esempio, se la cartella di backup è `C:/Program Files/ApacheGroup/Apache2/htdocs/backup`, il file `46xxsettings.txt` deve avere una linea simile a `SET BRURI http://www.example.com/backup`.

Prerequisiti

Procedura

1. Modificare il file di configurazione del server Web `httpd.conf`.
2. Togliere i simboli di commento dalle due righe `LoadModule` associate a DAV:
   - `LoadModule dav_module modules/mod_dav.so`
   - `LoadModule dav_fs_module modules/mod_dav_fs.so`

   Nota:

   se questi moduli non sono disponibili nel sistema in uso (in genere con alcuni server Unix/Linux Apache), sarà necessario ricompilare questi due moduli (mod_dav e mod_dav_fs) nel server. Potrebbero essere disponibili altri metodi per caricare i moduli. Per ulteriori dettagli, consultare la documentazione Apache a http://httpd.apache.org/docs/.
3. Aggiungere le righe seguenti al file `httpd.conf`:

```
#
Configurazione #WebDAV
#D
```

```
avLockDB "C:/Programmi/Gruppo Apache/Apache2/var/DAVLock"
<Location />
Dav On
</Location>
```

Nota:

Per i server Web Unix/Linux, la quarta riga può essere simile a: DavLockDB/usr/local/apache2/var/DAVLock

4. Creare la directory var e consentire a tutti di accedervi in scrittura. Fare clic con il pulsante destro del mouse **Proprietà** e selezionare **Sicurezza** > **Aggiungi** > **Tutti** > **Controllo completo** > **.**

Collegamenti correlati

File di esempio alla pagina 67

Parte 4: Procedure di installazione avanzate

Capitolo 12: Installazione dell'indirizzo statico

L'indirizzo statico è necessario solo se non è disponibile o non si intende utilizzare alcun server DHCP. Per facilità di manutenzione e installazione, verificare che venga utilizzato un server DHCP ed evitare indirizzi statici. Successivamente a un aggiornamento del file di avvio del firmware del telefono, le informazioni sull'indirizzo statico potrebbero richiedere una nuova installazione.

Collegamenti correlati

[Installazione dell'indirizzo statico per i telefoni serie 1600](#) alla pagina 72
[Impostazioni di installazione dell'indirizzo statico per le serie di telefoni 1600](#) alla pagina 73
[Installazione dell'indirizzo statico per i telefoni serie 9600](#) alla pagina 73
[Impostazioni di installazione dell'indirizzo statico per le serie di telefoni 9600](#) alla pagina 74

Installazione dell'indirizzo statico per i telefoni serie 1600

Procedura

1. Completare la procedura di connessione del telefono, e quando viene visualizzato `DHCP`, premere * per passare all'installazione dell'indirizzo statico.

   Il telefono visualizza una sequenza di impostazioni e il valore esistente per ognuna di queste impostazioni.

2. Per accettare i valori esistenti premere # oppure immettere un valore e quindi premere #. Consultare [Impostazioni di installazione dell'indirizzo statico per le serie di telefoni 1600](#) alla pagina 73.

   Nota:

   Se non viene modificato alcun valore, sul telefono viene visualizzato `Nessun nuovo valore`.

3. Se il telefono visualizza `Immetti`, spegnere e riaccendere il telefono.

   Dopo aver immesso tutti i valori o accettato i valori esistenti, il telefono visualizza `Salvare nuovi valori?`.

4. Per salvare i valori, premere #.

Passi successivi

Registrare il telefono.

Collegamenti correlati

Installazione dell'indirizzo statico alla pagina 72

Impostazioni di installazione dell'indirizzo statico per le serie di telefoni 1600

Nome delle impostazioni	Descrizione
Telefono	Questo è l'indirizzo IP del telefono. Per accettare il valore corrente premere # oppure immettere un valore e quindi premere #. Se si immette un nuovo valore, premere il tasto * per inserire un "." tra le cifre.
CallSv	Questo è l'indirizzo del gatekeeper H.323. Per i sistemi IP Office si tratta dell'indirizzo IP della LAN IP Office.
Porta server di chiamata	Questo è il numero della porta del livello di trasporto gatekeeper. Per i telefoni IP Avaya IP, il valore utilizzato è 1719. Per accettare il valore corrente premere # oppure immettere un valore e quindi premere #.
Router	Questo è l'indirizzo del gateway predefinito del telefono. Per IP Office questo è in genere l'indirizzo IP della LAN IP Office. Per accettare il valore corrente premere # oppure immettere un valore e quindi premere #.
Maschera	Questa è la maschera IP del telefono (anche detta Subnet Mask). La maschera IP viene utilizzata insieme all'indirizzo IP per indicare la subnet del telefono. È necessario che corrisponda alla maschera IP impostata per l'Unità IP Office.
FileSv	Questo è l'indirizzo del file server da cui il telefono deve richiedere il software e i file delle impostazioni. Immettere l'indirizzo TFTP o HTTP configurato con il set di file software per il telefono IP Avaya.
802.1Q	Premere * per cambiare l'impostazione. Premere # per accettare il valore.
ID VLAN	Per informazioni sulla configurazione VLAN, vedere VLAN e telefoni IP.

Collegamenti correlati

Installazione dell'indirizzo statico alla pagina 72

Installazione dell'indirizzo statico per i telefoni serie 9600

Procedura

1. Quando viene visualizzato `* da programmare`, premere il tasto *.
2. Se viene visualizzato `Immettere codice`, immettere il codice delle procedure amministrative e premere #. Il passcode predefinito è CRAFT (27238).

3. Scorrere fino a ADDR nel menu e selezionare questa opzione per avviare la procedura di impostazione dell'indirizzo.

   Viene visualizzato l'elenco di indirizzi richiesti. Se vengono visualizzati i valori del telefono esistenti. Se invece il telefono è nuovo o è stato formattato, tutti gli indirizzi sono impostati su 0.0.0.0.

4. Impostare ciascun indirizzo per evidenziare il valore da modificare e fare clic su **Cambia**. Vedere le impostazioni di installazione dell'indirizzo statico.
5. Immettere il nuovo valore per l'indirizzo, quindi selezionare **Salva**.
6. Quando tutti i valori sono impostati secondo necessità, fare clic su **Indietro** e quindi su **Esci**.

   Il telefono si riavvia utilizzando i nuovi valori.

Passi successivi

Registrare il telefono.

Collegamenti correlati

[Installazione dell'indirizzo statico](#) alla pagina 72

Impostazioni di installazione dell'indirizzo statico per le serie di telefoni 9600

Nome delle impostazioni	Descrizione
Telefono	Questo è l'indirizzo IP del telefono. Per accettare il valore corrente premere # oppure immettere un valore e quindi premere #. Se si immette un nuovo valore, premere il tasto * per inserire un "." tra le cifre.
Server di chiamata	Questo è l'indirizzo del gatekeeper H.323. Per i sistemi IP Office si tratta dell'indirizzo IP della LAN IP Office.
Router	Questo è l'indirizzo del gateway predefinito del telefono. Per IP Office questo è in genere l'indirizzo IP della LAN IP Office. Per accettare il valore corrente premere # oppure immettere un valore e quindi premere #.
Maschera	Questa è la maschera IP del telefono (anche detta Subnet Mask). La maschera IP viene utilizzata insieme all'indirizzo IP per indicare la subnet del telefono. È necessario che corrisponda alla maschera IP impostata per l'Unità IP Office.
File server HTTP	Questo è l'indirizzo del file server HTTP da cui il telefono deve richiedere il software e i file delle impostazioni.
Server file HTTPS	Questo è l'indirizzo del file server HTTPS da cui il telefono deve richiedere il software e i file delle impostazioni. Il telefono tenterà di utilizzare questo indirizzo, se impostato, prima di utilizzare l'HTTP.
802.1Q	Premere * per cambiare l'impostazione. Premere # per accettare il valore.
ID VLAN	Per informazioni sulla configurazione VLAN, vedere VLAN e telefoni IP.
Test VLAN	In caso di utilizzo della rete VLAN, si tratta del tempo di attesa (in secondi) di una risposta da parte del server DHCP nella rete VLAN prima che il telefono torni al normale utilizzo non VLAN.

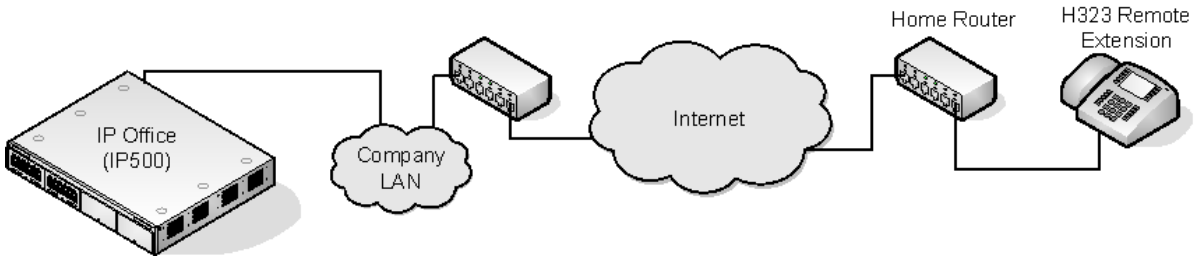
Collegamenti correlati

Installazione dell'indirizzo statico alla pagina 72

Capitolo 13: Interni H.323 remoti

Per la versione IP Office 8.0+ è supportata la configurazione di interni H.323 remoti, senza bisogno di particolari firmware VPN in esecuzione. Questa opzione è concepita per il seguente scenario:

- La LAN del cliente dispone di un indirizzo IP pubblico inoltrato al sistema IP Office. L'indirizzo viene utilizzato come indirizzo del server chiamate dagli interni H.323 remoti.
- L'utente dispone di un telefono H.323 dietro un router domestico. Si presuppone che il router domestico consenta tutto il traffico in uscita dalla rete domestica e tutto il traffico simmetrico. In altre parole, se il telefono invia RTP/RTCP a un indirizzo IP e una porta pubblici, sarà in grado di ricevere RTP/RTCP dallo stesso indirizzo IP e dalla stessa porta. Le configurazioni di altro tipo non sono illustrate in questo documento.



- Il sistema può essere configurato per supportare interni remoti H.323 nel caso venga utilizzato NAT nel percorso di connessione. Questa operazione può essere necessaria, ad esempio, se IP Office è protetto da un router/firewall NAT aziendale e/o il telefono H.323 è posizionato dietro un router NAT residenziale. L'utilizzo di questa opzione e l'interazione e la configurazione degli elementi esterni di terzi non rientrano nell'ambito della presente documentazione.
- Se l'indirizzo IP pubblico del router aziendale è sconosciuto, è necessario configurare un server STUN nelle impostazioni Topologia di rete della LAN di IP Office. Tuttavia, questa opzione non è supportata nel caso in cui Tipo di firewall/NAT sia impostato su Firewall simmetrico o Internet aperto.
- L'abilitazione dell'opzione Supporta interno remoto rende inoltre visibile la configurazione delle impostazioni dell'opzione Intervallo numeri porta (NAT) RTP.
- Telefoni supportati: Attualmente, l'utilizzo dell'interno H.323 remoto è supportato solo nei telefoni di serie 9600 già supportati dal sistema IP Office.
- Requisiti di licenza: Per impostazione predefinita è possibile configurare solo 4 utenti per l'utilizzo dell'interno H.323 remoto senza la necessità di licenze. È possibile configurare altri utenti se provvisti di licenza e configurati con i profili utente **Teleworker** o **Power User**.

Collegamenti correlati

[Configurazione della rete del cliente](#) alla pagina 77
[Configurazione del sistema IP Office](#) alla pagina 77

Configurazione Telefono alla pagina 79

Configurazione della rete del cliente

La LAN aziendale che ospita il sistema IP Office necessita di un indirizzo IP pubblico instradato all'interfaccia LAN del sistema IP Office configurato per il supporto dell'interno H.323 remoto.

Per determinare il tipo di NAT applicato al traffico tra il sistema e Internet, viene utilizzato il protocollo STUN dal sistema IP Office a Internet. Qualsiasi router o firewall tra la postazione telefonica H.323 e il sistema IP Office deve consentire il traffico indicato di seguito.

Protocollo	Porta	Descrizione
ICMP	-	Deve essere consentito il protocollo ICMP in entrata verso l'indirizzo IP pubblico del sistema IP Office.
UDP	1719	Deve essere consentito il traffico dalla porta UDP 1719 verso il sistema IP Office. Questa porta viene utilizzata per processi RAS H225 quali rilevazione gatekeeper, registrazione, keepalive e così via. Se questa porta non è aperta, il telefono non potrà effettuare la registrazione al sistema IP Office.
TCP	1720	Deve essere consentito il traffico dalla porta TCP 1720. Questa porta viene utilizzata per H.225 (segnalazione di chiamata). È possibile modificare l'indirizzo in uso mediante l'impostazione Porta di segnalazione delle chiamate remote.
RTP	Varie	Le porte nell'intervallo specificato dalle impostazioni Intervallo numeri porta (NAT) RTP del sistema devono essere consentite.
RTCP		
UDP	5005	Se è stata abilitata l'impostazione di sistema Abilita monitoraggio RTCP su porta 5005, è necessario consentire il traffico su questa porta per includere gli interni H.323 remoti nel monitoraggio.

Configurazione della rete dell'utente

Si presuppone che il router domestico consenta tutto il traffico in uscita dalla rete domestica e tutto il traffico simmetrico. In altre parole, se il telefono invia RTP/RTCP a un indirizzo IP e una porta pubblici, il router consente di ricevere RTP/RTCP dagli stessi indirizzo IP e porta.

Collegamenti correlati

Interni H.323 remoti alla pagina 76

Configurazione del sistema IP Office

Informazioni su questa attività

Di seguito è indicato un riepilogo delle modifiche di configurazione del sistema IP Office necessarie. In questa sezione si presuppone una conoscenza di base del sistema IP Office e dell'installazione del telefono IP H.323.

Prerequisiti

Se si devono supportare più di 4 utenti di interni remoti, il sistema deve prevedere licenze **Teleworker** e/o **Power User** disponibili per tali utenti.

Procedura

1. Nella scheda **Sistema**, configurare le impostazioni seguenti:
   a. Accedere a **Sistema** > **LAN1** > **LAN2** > **VoIP**.
   b. Abilitare la casella di controllo **Attivazione gatekeeper H323**.

      Nota:

      Considerando le ulteriori impostazioni necessarie alla configurazione di nuovi utenti e interni H.323 remoti, le voci utente e interno vengono aggiunte manualmente.

   c. Attivare **Attivazione interno remoto H.323**.
   d. Immettere il valore desiderato in **Porta di segnalazione delle chiamate remote**.

      Il valore predefinito 1720 corrisponde anche alla porta utilizzata dagli interni.

   e. Impostare **Intervallo numeri porta RTP (NAT)** in modo da racchiudere l'intervallo di porte da utilizzare per il traffico RTP e RTCP dell'interno H.323 remoto.

      Nota:

      L'intervallo impostato deve fornire almeno due porte supportate per interno.

2. Nella scheda **Topologia di rete**, configurare le impostazioni seguenti:

   Nota:

   È possibile utilizzare il protocollo STUN per determinare il tipo dei processi NAT/ firewall applicati al traffico tra il sistema IP Office e Internet.

   a. Andare su **Topologia di rete** e impostare **Indirizzo IP server STUN** su un server STUN noto.
   b. Fare clic su **OK**

      Il pulsante **Esegui STUN** è abilitato.

   c. Fare clic su **Esegui STUN** e attendere che il processo STUN venga eseguito.

      I risultati rilevati dal processo vengono indicati dalle icone ! accanto ai campi.

   d. Se STUN segnala **Tipo di firewall/NAT**, la rete deve essere riconfigurata.

      Nota:

      I tipi di rete **Blocco porta statico**, **NAT simmetrico** o **Internet aperto** non sono supportati per gli interni H.323 remoti.

3. Nella scheda **Utente**, configurare le impostazioni seguenti:
   a. Accedere alla scheda **Utente**, impostare **Profilo utente** su **Teleworker** o **Power User**.
   b. Attivare **Abilita Remote Worker**.

Collegamenti correlati

Interni H.323 remoti alla pagina 76

Configurazione Telefono

I telefoni non richiedono un firmware particolare. Per questo motivo vengono prima installati come normali interni, quindi, durante il processo di installazione, caricano il firmware fornito dal sistema IP Office.

Una volta completato il processo, le impostazioni relative all'indirizzo del telefono devono essere eliminate e l'indirizzo del server chiamate impostato sull'indirizzo pubblico utilizzato dagli interni H.323 remoti.

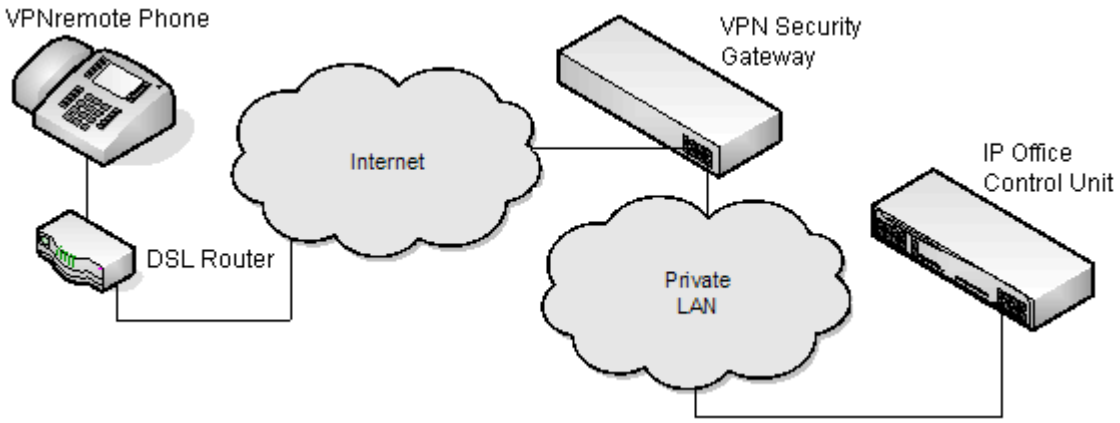
Si presuppone che, nelle postazioni in remoto, il telefono ottenga le altre informazioni relative all'indirizzo tramite il DHCP del router dell'utente. Se non è questo il caso, è necessario amministrare in modo statico le altre impostazioni relative all'indirizzo per trovare indirizzi adatti alla rete domestica dell'utente.

Collegamenti correlati

Interni H.323 remoti alla pagina 76

Capitolo 14: Telefoni remoti VPN

I telefoni IP Avaya in postazioni remote possono essere collegati al sistema IP Office tramite tunnel VPN IPSec. Questa opzione è supportata per i telefoni 4610SW, 4621SW, 5610SW e 5621SW. È supportata anche per i telefoni della serie 9600.



Di seguito sono indicati ulteriori componenti richiesti per i telefoni remoti tramite VPN:

- Firmware del telefono IP Office VPNremote: il firmware è incluso nel set di firmware del telefono IP.
- Gateway di sicurezza VPN: il sistema IP Office non supporta tutte le funzionalità IPSec necessarie per i telefoni VPNremote che utilizzano specifici tunnel IPSec. Per questo motivo è necessario che il tunnel VPN dei telefoni remoti termini in un dispositivo gateway VPN alternativo. Il dispositivo deve supportare uno dei metodi elencati di seguito:
  - Gateway Avaya: dispositivi gateway di protezione Avaya (SG e VSU) che utilizzano un protocollo proprietario denominato
    - serie CCD SG Avaya (versione del firmware 4.6 o superiore)
    - Serie VSU Avaya (versione del firmware 3.2 o superiore)
  - Gateway non Avaya: gateway VPN non Avaya con autenticazione estesa IKE (Xauth) e chiave già condivisa (PSK). Sono disponibili note per l'installazione degli elementi elencati di seguito. Mettendo a disposizione tali indicazioni, Avaya non intende in alcun modo consigliarne l'adozione o precludere l'utilizzo di altri dispositivi.

    Nota:

    Avaya non garantisce il supporto dei servizi forniti tramite dispositivi non Avaya.

    - Concentratori Cisco VPN 300
    - Dispositivi di protezione Cisco PIX 500

- Dispositivi Juniper Networks NetScreen VPN
- SSG (Secure Services Gateway) Juniper Networks serie 500
- Gateway di protezione integrata (ISG) Juniper Networks
- Router VPN Kentrox Q2300
- Router VPN Sonicwall Tz170
- Router VPN Netgear FVS338
- Router VPN Netgear FVX538
- Router VPN Adtran Netvanta 3305

Collegamenti correlati

Documentazione di installazione alla pagina 81
Firmware del telefono remoto VPN supportato alla pagina 81
Configurazione del telefono IP per VPN remote alla pagina 82
VLAN e telefoni IP alla pagina 82
VLAN e DHCP alla pagina 84
Configurazione di esempio - Panoramica alla pagina 85
Panoramica di un sistema d'esempio alla pagina 87

Documentazione di installazione

Questo documento fornisce indicazioni e note sulle differenze specifiche dell'installazione di telefoni VPNremote con IP Office. In seguito, la procedura di installazione e configurazione dei telefoni VPNremote Avaya è descritta in una serie di documenti esistenti disponibili sul sito web dell'assistenza Avaya (http://support.avaya.com). Fare riferimento alla *Guida alla configurazione VPN per i telefoni IP serie 9600* rif. documentazione *16-602968*.

Collegamenti correlati

Telefoni remoti VPN alla pagina 80

Firmware del telefono remoto VPN supportato

Se non altrimenti specificato, utilizzare solo il firmware fornito sul DVD delle applicazioni per l'amministratore IP Office per i telefoni VPNremote collegati a un sistema IP Office. Il firmware è stato testato con la versione IP Office per verificarne il corretto funzionamento. Il firmware è contenuto all'interno di un file zip nella cartella `\bin\VPN Phone`.

Eventuali altre versioni del firmware VPNremote rese disponibili da Avaya in futuro potrebbero non essere specificamente testate per IP Office.

Collegamenti correlati

Telefoni remoti VPN alla pagina 80

Configurazione del telefono IP per VPN remote

Informazioni su questa attività

Inoltre, nella scheda delle impostazioni degli interni IP **Interno** > **VoIP**, è disponibile la casella di controllo Telefono VPN Consentito. La casella di controllo **VoIP** consente di indicare a IP Office quali sono gli interni IP VPNremote, che richiedono pertanto una licenza.

Procedura

1. Utilizzando IP Office Manager, recuperare la configurazione dal sistema.
2. Fare clic su **Interno** e selezionare la voce dell'interno IP.
3. Selezionare il tab **VoIP**.
4. Attivare **Telefono VPN consentito**.
5. Fare clic su **OK**.
6. Ripetere la procedura per gli altri interni IP da convertire alla connessione VPN.
7. Salvare la configurazione.

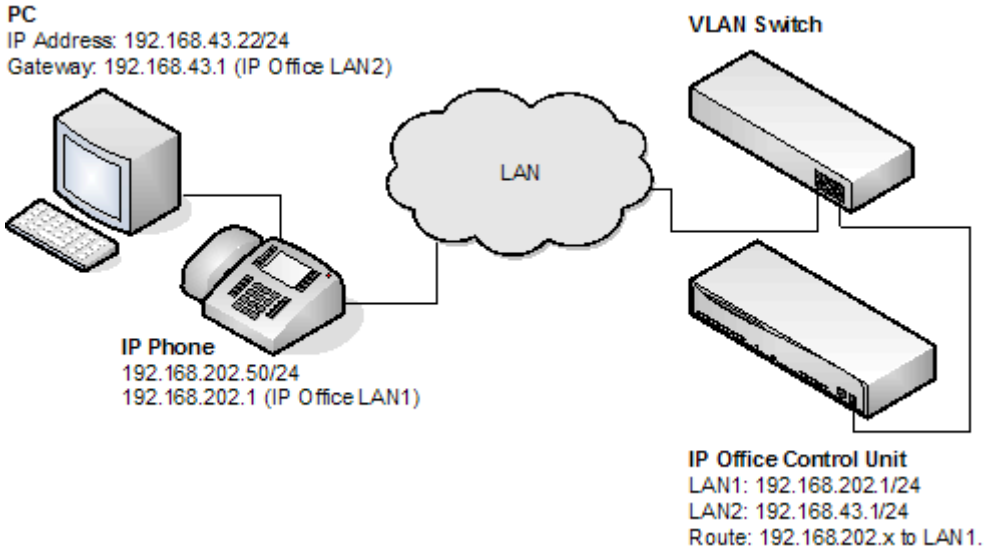
Collegamenti correlati

Telefoni remoti VPN alla pagina 80

VLAN e telefoni IP

L'utilizzo della VLAN consente di creare domini di collisione separati sugli switch Ethernet. Nel caso di IP Office e dei telefoni IP i vantaggi includono:

- Possibilità per i PC di continuare nella stessa subnet IP, mentre i telefoni IP possono utilizzare uno schema nuovo e separato di indirizzi IP.
- Non viene propagato traffico broadcast tra la rete dati del PC e la rete vocale dei telefoni IP. Ciò consente di migliorare le prestazioni dal momento che il traffico broadcast deve essere valutato da tutti i ricevitori.
- La rete VLAN e la definizione delle priorità del traffico sul livello 2 sono strettamente associate nello stesso standard 802.2. È quindi più facile gestire la QoS L2 in caso di utilizzo di una rete VLAN.



La tabella mostra i tre modi in cui è possibile implementare una VLAN con uno switch Ethernet. I primi due metodi richiedono solo una configurazione elementare. In questo documento l'attenzione verrà concentrata sul terzo metodo (sovrapposizione) in quanto si dà per scontato che il PC e i telefoni IP condividano la stessa porta Ethernet.

Tipo	Descrizione	Vantaggi	Svantaggi
Senza VLAN	Voce e dati occupano lo stesso dominio di collisione	Configurazione semplice	Il traffico di trasmissione del PC influenza negativamente il traffico vocale. Richiede due (2) porte per utente, una per il telefono IP e l'altra per il PC
VLAN fisica	VLAN separata per dati e voce	Configurazione semplice	Richiede due (2) porte sullo switch, una per il telefono IP e l'altra per il PC.
Sovrapposizione della VLAN	Su un'unica porta nello switch viene trasmesso sia il traffico dei telefoni IP che quello del PC	Richiede un'unica porta per il PC e il telefono IP Il traffico di trasmissione del PC non può incidere in modo negativo sul traffico vocale	Configurazione complessa

Collegamenti correlati

[Telefoni remoti VPN](#) alla pagina 80

VLAN e DHCP

L'utilizzo della VLAN comporta alcune conseguenze su DHCP, se viene utilizzato per supportare telefoni IP e/o PC. Nella tabella indicata di seguito vengono riportate nel dettaglio le opzioni disponibili in caso di utilizzo di un'unica porta per PC e telefoni IP in una rete abilitata VLAN.

Opzione DHCP	Descrizione
Nessuno (indirizzo statico)	Configurazione manuale di ciascun telefono IP
Server DHCP separati	Due PC, uno per ogni VLAN
Server DHCP con multihoming	Un unico PC con due schede NIC, una per ogni VLAN
Relè DHCP	L'opzione deve essere supportata dallo switch Ethernet

Se si utilizza il DHCP, al momento dell'avvio del telefono IP, questo eseguirà in primo luogo una richiesta DHCP senza tag VLAN.

- Se la risposta DHCP contiene una nuova impostazione VLAN nell'ambito del numero opzione specifico per sito (SSON), i telefoni rilasceranno gli indirizzi IP esistenti e verrà effettuata una nuova richiesta DHCP mediante l'ID VLAN appena fornito

  Se il telefono IP non ottiene un nuovo ID VLAN, continuerà a utilizzare le impostazioni fornite nella risposta DHCP originale

È inoltre possibile passare un ID VLAN a un telefono utilizzando il file di impostazioni caricato. Il telefono IP rilascerà nuovamente tutti i parametri IP esistenti, quindi verrà effettuata una nuova richiesta DHCP mediante l'ID VLAN appena fornito.

Nell'esempio indicato di seguito, nel momento in cui i telefoni IP ricevono una risposta DHCP dal server DHCP nella VLAN dei dati, la risposta conterrà l'ID VLAN della VLAN vocale. Il telefono rilascerà quindi le impostazioni originali della VLAN dati ottenute e verrà inviata una nuova richiesta DHCP alla VLAN vocale.

Opzione	Impostazioni DHCP della VLAN dati	Impostazioni DHCP della VLAN vocale
Indirizzo IP	192.168.43.x	192.168.202.x
Maschera	255.255.255.0	255.255.255.0
Router	192.168.43.1	192.168.202.1
SSON Ambito	L2Q=1, L2QVLAN=202, VLANTEST=0	MCIPADD=192.168.202.1, MCPORT=1719, HTTPSRVR=192.168.202.X VLANTEST=0
Il parametro VLANTEST è l'intervallo di tempo in cui il telefono IP deve effettuare richieste DHCP in una VLAN (0 significa tempo illimitato).		

Collegamenti correlati

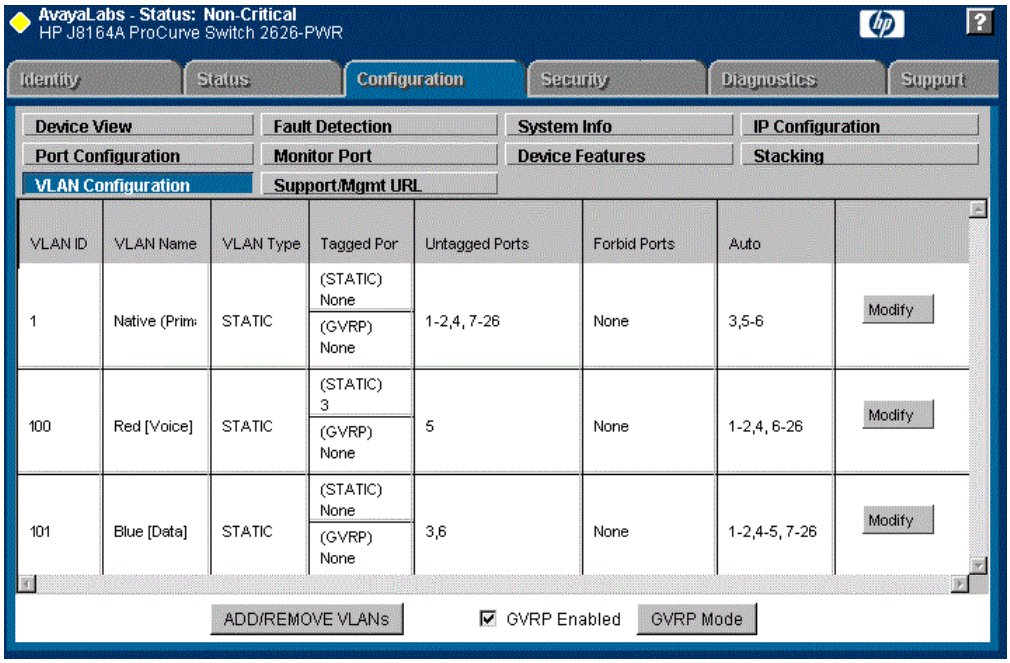
Telefoni remoti VPN alla pagina 80

Configurazione di esempio - Panoramica

La rete è stata ideata per consentire al PC dell'utente di collegarsi alla porta dello switch del telefono IP. Un cavo unico collega quindi il PC e il telefono IP allo switch Ethernet. Per questo esempio vengono utilizzate la rete VLAN 100 per il traffico vocale e la rete VLAN 101 per il traffico dati. L'interfaccia LAN1 dell'unità di controllo IP Office risiede nella VLAN voce mentre l'interfaccia LAN2 risiede nella VLAN dati. Le comunicazioni tra la VLAN voce e quella dati vengono facilitate dalle funzionalità router dell'unità di controllo IP Office.

HP-Switch - Configurazione

Di seguito vengono mostrati gli output delle configurazioni Web e CLI dallo switch HP Procurve. Gli output sono stati ricavati dalle linee guida di configurazione indicate di seguito.



HP Procurve CLI output

```
; J8164A Configuration Editor; Created on release #H.08.60

hostname "AvayaLabs"
snmp-server community "public" Unrestricted
vlan 1
name "Native"
untagged 1-2,4,7-26
ip address 192.168.202.201 255.255.255.0
no untagged 3,5-6
exit
vlan 100
name "Red [Voice]"
untagged 5
tagged 3
exit
vlan 101
name "Blue [Data]"
untagged 3,6
exit
gvrp
spanning-tree
```

Nella tabella indicata di seguito viene fornito un riepilogo della configurazione HP per le porte e le reti VLAN.

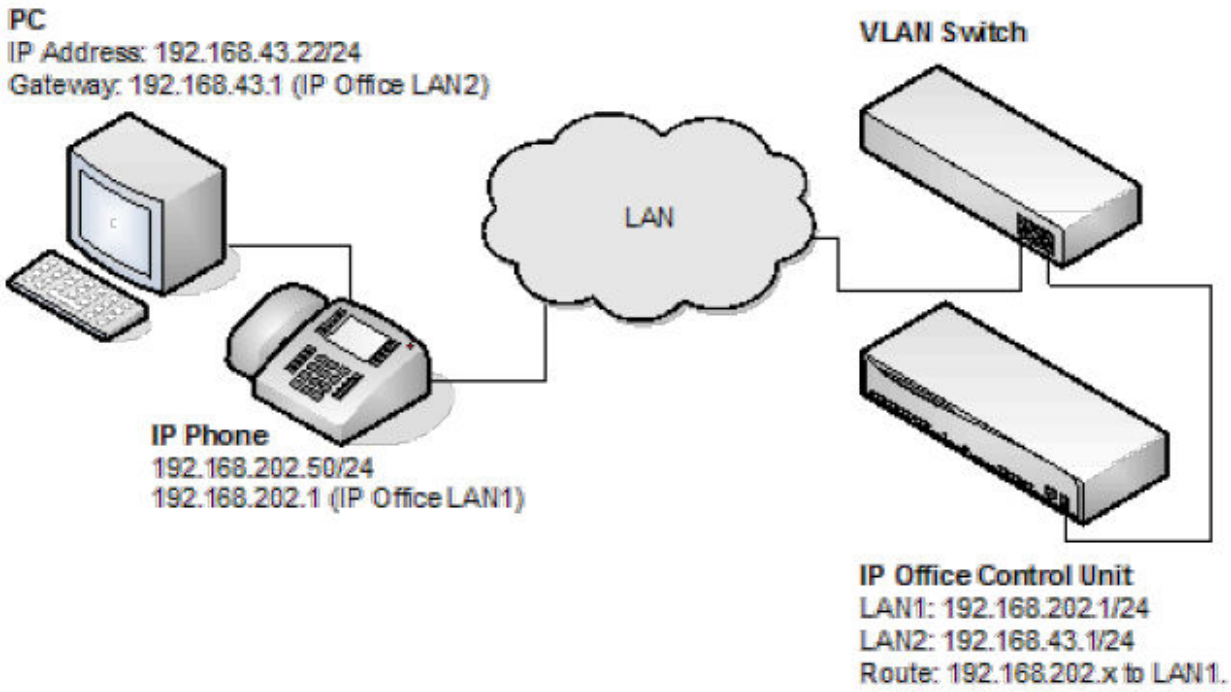
Porta	VLAN 100 Voce	VLAN 101 Dati	Descrizione
3	Con tag	Senza tag	Questa porta è stata aggiunta a entrambe le reti VLAN 100 e VLAN 101. **Nota:** in caso di aggiunta della porta 3 alla rete VLAN 100, è necessario assegnare tag all'opzione Modalità (i tag dovranno essere rimossi in caso di aggiunta alla rete VLAN 101).
5	Senza tag	-	Questa porta viene inclusa solo nella VLAN 100 e non nella VLAN 101. È necessario che l'opzione Modalità sia impostata su Senza tag per la porta 5 in questa VLAN.
6	-	Senza tag	La porta 6 viene inclusa solo nella VLAN 101 e non nella VLAN 100. È necessario che l'opzione Modalità sia impostata su Senza tag in questa VLAN.

Il funzionamento di questa rete dipende dalla funzionalità definita nella documentazione HP. In particolare HP si riferisce a questo tipo di funzionamento della VLAN come **Sovrapposizione della VLAN**.

Collegamenti correlati

Telefoni remoti VPN alla pagina 80

Panoramica di un sistema d'esempio



- Configurazione IP Office: La tabella seguente illustra dettagliatamente la configurazione di IP Office. Per il supporto del tagging 802.1 IP Office non richiede configurazioni aggiuntive.

Opzione	Valore
LAN1 indirizzo IP	192.168.202.1
LAN1 maschera IP	255.255.255.0
LAN2 indirizzo IP	192.168.43.1
LAN2 maschera IP	255.255.255.0
Router	192.168.202.1
Server di chiamata	192.168.202.1

- Configurazione Telefono IP: Nell'esempio indicato di seguito il telefono IP è stato configurato con un indirizzo IP fisso.

Opzione	Valore
Indirizzo IP	192.168.202.50
Maschera IP	255.255.255.0
Router	192.168.202.1
Server di chiamata	192.168.202.1
VLANID	100

- Configurazione Switch VLAN: Nella tabella indicata di seguito viene fornito un riepilogo della configurazione HP per le porte e le reti VLAN.

Porta	VLAN 100 Voce	VLAN 101 Dati
3	Con tag	Senza tag
5	Senza tag	-
6	-	Senza tag

- Configurazione del PC: Di seguito viene illustrata la configurazione IP del PC1; sul PC non è stata attivata alcuna opzione per il supporto di 802.1q o 802.1p.

Opzione	Valore
Indirizzo IP	192.168.43.22
Maschera IP	255.255.255.0
Router	192.168.43.1

Riepilogo

Dalla porta in cui risiedono il PC e il telefono IP possono essere ricevuti due tipi di frame Ethernet (che vengono inviati dal telefono o dal PC):

- I pacchetti che dispongono di tag vengono inviati dal telefono IP.
- I pacchetti sprovvisti di tag vengono inviati dal PC.

Quando un pacchetto senza tag viene inviato dal PC collegato alla porta del telefono IP, verrà propagato solo alla VLAN 101. Ciò avviene perché, quando si è aggiunta la porta 3 alla VLAN 101, l'opzione **Modalità** è stata specificata come senza tag. Per l'altra VLAN (101), invece, è stata selezionata l'opzione **Con tag** per la porta 3 nella VLAN 101. Pertanto i pacchetti con tag verranno destinati alla VLAN 100, mentre quelli senza tag alla VLAN 101.

Se il pacchetto viene originato da un telefono IP dispone di tag. Dal momento che l'opzione "Senza tag" è stata selezionata per la porta 5 nella VLAN 100, il tag 802.1 viene rimosso prima che lo switch inoltri il pacchetto a questa porta. In modo analogo, quando un pacchetto senza tag viene originato e inviato da IP Office, lo switch attribuirà un tag al pacchetto prima di inoltrarlo alla porta 3 della LAN.

Collegamenti correlati

Telefoni remoti VPN alla pagina 80

Capitolo 15: Configurazione di un server DHCP alternativo

Il metodo di installazione consigliato per i telefoni IP H.323 prevede l'utilizzo di un server DHCP. In questa sezione viene delineata a titolo esemplificativo la procedura di base per l'utilizzo di un server Windows come server DHCP per l'installazione del telefono IP. I principi di definizione di un ambito sono applicabili alla maggior parte dei server DHCP.

L'utente avrà bisogno delle informazioni riportate di seguito dall'amministratore di rete del cliente:

- L'intervallo degli indirizzi IP e la subnet mask che dovranno utilizzare i telefoni IP H.323
- l'indirizzo del gateway IP
- il nome di dominio DNS, l'indirizzo del server DNS e l'indirizzo del server WINS
- la durata del lease DHCP
- L'indirizzo IP dell'unità IP Office
- L'indirizzo IP del PC su cui è in esecuzione Manager (questo PC agisce da server dei file per i telefoni IP H.323 durante l'installazione)

Collegamenti correlati

Opzioni alternative alla pagina 89
Controllo del supporto del server DHCP alla pagina 91
Creazione di un ambito alla pagina 91
Aggiunta dell'opzione 242 alla pagina 93
Attivazione dell'ambito alla pagina 94

Opzioni alternative

In questo documento, tutte le informazioni sul telefono IP vengono pubblicate tramite l'ambito e le impostazioni relative all'Opzione 176 o 242. Potrebbero essere state utilizzate altre opzioni all'interno dell'ambito, a seconda del server DHCP.

Opzione	Descrizione
Opzione 1 - Maschera di sottorete	

La tabella continua…

Opzione	Descrizione
Opzione 3 - Indirizzo IP gateway	Se si utilizza più di un indirizzo, l'elenco completo può contenere fino a un massimo di 255 caratteri ASCII. Gli indirizzi IP devono essere separati da virgole, senza spazi.
Opzione 6 - Indirizzo server DNS	Se si utilizza più di un indirizzo, l'elenco completo può contenere fino a un massimo di 127 caratteri ASCII. Gli indirizzi IP devono essere separati da virgole, senza spazi. L'Opzione 6 deve includere almeno un indirizzo valido, diverso da zero, con decimali puntati.
Opzione 15 - Nome dominio DNS	Questa stringa contiene il nome di dominio da utilizzare quando i nomi DNS nei parametri di sistema vengono risolti in indirizzi IP. Questo nome di dominio viene accodato al nome DNS prima che il telefono IP tenti di risolvere l'indirizzo DNS. L'Opzione 15 è necessaria se si intende utilizzare un nome DNS per il server HTTP.
Opzione 51 - Lease time del DHCP	Se non viene ricevuta questa opzione, l'offerta DHCP non verrà accettata. Avaya consiglia di utilizzare un lease time di almeno sei (6) settimane. Se questa opzione ha un valore di FFFFFFFF hex, si presume che il lease dell'indirizzo IP sia pari a infinito, come specificato in RFC 2131, Sezione 3.3, affinché le procedure di rinnovo e rebinding non siano necessarie anche se vengono ricevute le Opzioni 58 e 59. I lease scaduti provocano il riavvio dei telefoni IP Avaya. • Prevedere un numero di lease sufficiente per evitare la variazione dell'indirizzo IP di un telefono IP se il telefono risulta offline per un breve periodo di tempo. • Lo standard DHCP prevede che alla scadenza di un lease DHCP il dispositivo smetta immediatamente di utilizzare l'indirizzo IP assegnato. Se si verificano problemi di rete e l'unico server DHCP è centralizzato, il telefono non potrà accedere al server. In tal caso, il telefono non potrà essere utilizzato finché non sarà in grado di accedere al server. • Dopo aver assegnato un indirizzo IP, fare in modo che il telefono continui a utilizzare lo stesso indirizzo dopo la scadenza del lease DHCP, finché non viene rilevato un conflitto con un altro dispositivo. Il parametro personalizzabile DHCPSTD del telefono IP serie 1600 consente agli amministratori di specificare se il telefono: - È conforme allo standard DHCP impostando il parametro DHCPSTD su 1. - Deve continuare a utilizzare il proprio indirizzo IP dopo la scadenza del lease DHCP impostando il parametro DHCPSTD su 0. Questa funzione è predefinita. Se si utilizza questa impostazione, dopo la scadenza del lease DHCP il telefono invierà una richiesta ARP del proprio indirizzo IP ogni cinque (5) secondi. La richiesta viene ripetuta continuamente o fino a quando il telefono non riceve una risposta ARP. Una volta ricevuta la risposta ARP, il telefono visualizza un messaggio di errore, imposta il proprio indirizzo IP su 0.0.0.0 e tenta nuovamente di contattare il server DHCP.
Opzione 52 - Opzione di overload	Se viene ricevuta questa opzione in un messaggio, il telefono interpreta i campi del nome e del campo in base a quanto specificato in IETF RFC 2132, Sezione 9.3 (vedere l'Appendice B: Documentazione correlata).
Opzione 53 - Tipo di messaggio DHCP	Il valore può essere 1 (DHCPDISCOVER) o 3 (DHCPREQUEST).

La tabella continua…

Opzione	Descrizione
Opzione 55 - Elenco richiesta parametri	I valori accettabili sono: 1 (maschera di sottorete), 3 (indirizzo/i IP router), 6 (indirizzo/i IP DNS), 15 (nome di dominio), NVSSON (numero opzione sito specifico)
Opzione 57 - Dimensioni massime messaggio DHCP	Utilizzato da un client o server DHCP per specificare le dimensioni massime del messaggio DHCP che è disposto ad accettare.
Opzione 58 - Tempo di rinnovo lease DHCP	Se questo valore non viene ricevuto o se è maggiore del valore dell'Opzione 51, verrà utilizzato il valore predefinito di T1 (timer di rinnovo), come specificato in IETF RFC 2131, Sezione 4.5.
Opzione 59 - Tempo di rebinding lease DHCP	Se questo valore non viene ricevuto o se è maggiore del valore dell'Opzione 51, verrà utilizzato il valore predefinito di T2 (timer di rebinding), come specificato in IETF RFC 2131, Sezione 4.5

Nota:

nei telefoni IP H.323, le voci TFTP nell'Opzione 176 avranno la priorità sulle impostazioni dell'Opzione 66. L'utilizzo dell'Opzione 66 come parte dell'ambito risulta utile se vengono richiesti indirizzi gatekeeper alternativi nelle impostazioni dell'Opzione 176 e si mantiene il limite dei caratteri entro 127.

Collegamenti correlati

Configurazione di un server DHCP alternativo alla pagina 89

Controllo del supporto del server DHCP

Procedura

1. Sul server , selezionare **Avvia** > **Programmi** > **Strumenti di amministrazione** > **Gestione del computer**.
2. In **Servizi e applicazioni** nella struttura di gestione del computer, individuare **DHCP**.
3. Se DHCP non è presente, sarà necessario installare i componenti DHCP. Fare riferimento alla documentazione di Microsoft.

Passi successivi

Se è supportato il ruolo server DHCP, la prima fase consiste nel creare un ambito di indirizzi per l'utilizzo nei telefoni IP.

Collegamenti correlati

Configurazione di un server DHCP alternativo alla pagina 89

Creazione di un ambito

Informazioni su questa attività

Un ambito DHCP definisce gli indirizzi IP che i server DHCP possono emettere in risposta a richieste DHCP. È possibile definire ambiti diversi per tipi diversi di dispositivi.

Procedura

1. Accedere a **Avvia** > **Programmi** > **Strumenti di amministrazione** > **DHCP**
2. Fare clic con il tasto destro sul server e selezionare **Nuovo** > **Ambito**
3. Verrà avviata la procedura guidata dell'ambito, fare clic su **Avanti**.
4. Immettere un nome e un commento per l'ambito e fare clic su **Avanti**.
5. Immettere l'intervallo di indirizzi da utilizzare, ad esempio da 200.200.200.1 a 200.200.200.15 (la parte host non può essere 0).
6. Immettere la subnet mask o il numero di bit utilizzati o la maschera effettiva, ad esempio 24 è uguale a 255.255.255.0, e fare clic su **Avanti**.
7. È possibile specificare gli indirizzi da escludere. A tale scopo, immettere un intervallo e fare clic su **Aggiungi**.

   È possibile immettere un intervallo compreso tra 200.200.200.5 e 200.200.200.7

   Nota:

   È opportuno escludere IP Office dall'intervallo, in quanto le Opzioni DHCP in IP Office dovrebbero essere state disabilitate. Queste procedure vengono indicate solo a scopo di suggerimento. È possibile eseguire questa operazione anche lasciando gli indirizzi disponibili fuori dall'intervallo dell'ambito.
8. Fare clic su **Avanti**.
9. Impostare la durata del lease per gli indirizzi.

   Se viene impostata una durata troppo lunga, gli indirizzi utilizzati dai dispositivi non più connessi non scadranno e non potranno essere riutilizzati per un certo periodo di tempo. In questo modo viene ridotto il numero di indirizzi disponibili per i nuovi dispositivi. Se viene impostata una durata troppo breve, verrà generato traffico inutile per il rinnovo degli indirizzi. Il valore predefinito è di 8 giorni.
10. Fare clic su **Avanti**.
11. La procedura guidata presenta le opzioni per la configurazione delle opzioni DHCP più comuni. Selezionare **Sì**, quindi fare clic su **Avanti**.
12. Immettere l'indirizzo del gateway e fare clic su **Aggiungi**.
13. Fare clic su **Avanti**.
14. Immettere il dominio DNS (ad es. example.com) e gli indirizzi del server DNS e fare clic su **Avanti**.
15. Immettere gli indirizzi dei server WINS, fare clic su **Aggiungi**, quindi fare clic su **Avanti**.
16. A questo punto verrà richiesto se si desidera attivare l'ambito. Selezionare **No**, quindi fare clic su **Avanti**.
17. Fare clic su **Fine**.

Risultato

Il nuovo ambito verrà inserito nell'elenco e lo stato sarà impostato su **Inattivo**.

Una volta creato l'ambito che verrà utilizzato nei telefoni IP, sarà necessario aggiungere un set di opzioni corrispondenti al numero opzione specifico per sito (SSON) che verrà utilizzato dai

telefoni. Per impostazione predefinita, il numero SSON utilizzato dai telefoni della serie 1600 e 9600 è 242.

Collegamenti correlati

Configurazione di un server DHCP alternativo alla pagina 89

Aggiunta dell'opzione 242

Informazioni su questa attività

Oltre a emettere informazioni sugli indirizzi IP, i server DHCP sono in grado di emettere altre informazioni in risposta alle richieste dei diversi numeri di opzione specifici del DHCP. Le impostazioni di ciascuna opzione sono collegate all'ambito. I telefoni IP H.323 di serie 1600 e 9600 utilizzano il numero opzione specifico per sito (SSON) 242 per richiedere ulteriori informazioni da parte di un server DHCP. L'opzione deve includere la definizione dell'indirizzo del gatekeeper H.323 del telefono (IP Office) e l'indirizzo del server dei file HTTP.

Procedura

1. Fare clic con il tasto destro sul server DHCP.
2. Dal menu pop-up, selezionare **Opzioni predefinite**.
3. Selezionare **Aggiungi**.
4. Inserire le informazioni seguenti:
   a. In **Nome** immettere `16xxOptions`.
   b. In **Tipo dati** immettere `Stringa`.
   c. In **Codice** immettere `242`.
   d. In **Descrizione** immettere le impostazioni del telefono `IP`.
5. Fare clic su **OK**.
6. Nel campo del valore stringa, immettere `MCIPADD=xxx.xxx.xxx,MCPORT=1719,HTTPSRVR=yyyy.yyy.yyy,HTTPDIR=z,VLANTEST=0`.

   - La lunghezza massima della stringa è pari a 127 caratteri. Per ridurre la lunghezza, è possibile specificare l'indirizzo del server TFTP collegando una voce dell'Opzione 66 all'ambito. Consultare Opzioni alternative alla pagina 89.

     `MCIPADD=` è l'indirizzo del gatekeeper H.323 (Callserver). In genere, corrisponde all'indirizzo LAN1 dell'unità IP Office. È possibile immettere diversi indirizzi IP separandoli con una virgola e senza spazi. Questa operazione consente la specifica di gatekeeper H.323 di fallback. i telefoni attenderanno tre (3) minuti prima di passare al fallback e non torneranno alla modalità precedente quando viene ripristinato il primo server, fino al riavvio del telefono.
   - `MCPORT=` è l'indirizzo della porta RAS per l'inizializzazione della registrazione del telefono. La porta predefinita è la 1719.
   - `HTTPSRVR=` è l'indirizzo IP del file server HTTP.

- `HTTPDIR=` la directory file HTTP in cui si trovano i file del telefono IP. Questa voce non è obbligatoria se i file si trovano nella directory principale del server.

7. Fare clic su **OK**
8. Espandere il server facendo clic sul simbolo [+] adiacente.
9. Fare clic sull'ambito appena creato per i telefoni di serie 1600 e 9600.
10. Nel pannello a destra, fare clic con il pulsante destro del mouse sull'ambito e selezionare **Opzioni ambito**.
11. Nella scheda Generale, assicurarsi che sia selezionata l'Opzione 242.
12. Verificare che il valore Stringa sia corretto, quindi fare clic su **OK**.

Passi successivi

Una volta creata un'opzione 242 e associata all'ambito desiderato per l'utilizzo nei telefoni IP, procedere con l'attivazione dell'ambito

Collegamenti correlati

Configurazione di un server DHCP alternativo alla pagina 89

Attivazione dell'ambito

È possibile attivare l'ambito manualmente facendo clic con il tasto destro sull'ambito, selezionando **Tutte le attività** e selezionando **Attiva**. L'attivazione è immediata.

È ora possibile avviare l'installazione dei telefoni IP H.323 utilizzando DHCP. Se Manager viene utilizzato come server HTTP o TFTP, verificare che sia in esecuzione sul PC specificato.

Collegamenti correlati

Configurazione di un server DHCP alternativo alla pagina 89

Capitolo 16: Supporto SRTP

Per IP Office versione 9.1, l'SRTP è supportato.

- Modalità IP Office supportate: SRTP è supportato in tutte le modalità IP Office.
- Telefoni supportati: Applicabile agli interni SIP e H323. Tuttavia, potrebbero sussistere alcune limitazioni per determinati modelli di telefoni IP.
  - Supporto di H323 nei telefoni serie 9608, 9611, 9621 e 9641.
  - Supporto di SIP nei telefoni Avaya e di terze parti.
- Trunk supportati: Applicabile a tutti i tipi di linea IP (SIP, SM e IP Office (SCN)), tranne per i trunk H323 esterni.
- Licenze e Capacità: L'utilizzo di SRTP non richiede licenze o sottoscrizioni. Tuttavia, l'utilizzo di SRTP influisce sulla capacità di chiamata del sistema.
  - Per i sistemi IP500 V2/IP500 V2A dotati di schede VCM IP500, queste ultime vengono utilizzate per il supporto SRTP e attenuano le conseguenze sulla capacità di chiamata del sistema. Ciò non è valido per le schede combinazione.

Collegamenti correlati

Attivazione dell'SRTP di sistema alla pagina 95
Direct media alla pagina 97

Attivazione dell'SRTP di sistema

Per impostazione predefinita, tutti gli interni e le linee IP sono configurati per la corrispondenza automatica con le impostazioni di sistema di livello superiore, indipendentemente dal fatto che siano abilitate o disabilitate. Ciò semplifica l'abilitazione dell'SRTP, facendo in modo che tutti i dispositivi utilizzino le stesse impostazioni SRTP. Grazie a questo metodo, una volta abilitato l'SRTP, l'unica configurazione a livello dei dispositivi richiesta è la disabilitazione dell'SRTP nelle linee o nei dispositivi in cui questo non sia necessario.

L'eccezione a quanto indicato in precedenza è rappresentata dalle linee SIP, in cui l'SRTP è disabilitato per impostazione predefinita. Il motivo è il numero ridotto di fornitori di linee SIP che al momento supportano l'SRTP. Tuttavia, è possibile configurare le linee SIP per la corrispondenza delle impostazioni a livello di sistema, se necessario.

Collegamenti correlati

Supporto SRTP alla pagina 95
Abilitazione dell'SRTP di sistema alla pagina 96
Disattivazione di SRTP su un interno o una linea alla pagina 96

Abilitazione dell'SRTP di sistema

Procedura

1. Ricevere la configurazione dal sistema.
2. Fare clic su **Sistema** e selezionare la scheda **Sicurezza VoIP**.
3. Per **Sicurezza supporti**, selezionare il livello di operazione STRP richiesto:

Impostazione	Descrizione
Disabilitato	L'SRTP non viene utilizzato per le connessioni.
Massime risorse	Supporto di RTP e SRTP. Utilizzare SRTP se le impostazioni SRTP corrispondenti possono essere negoziate con il terminale remoto. Ciò richiede che l'entità finale remota supporti srtp rfc5939 (negoziazione della funzionalità per SRTP). Altrimenti, utilizzare RTP. I telefoni E129 non supportano **Massime risorse**.
Applicato	Utilizzare solo SRTP. Se l'entità finale remota non supporta l'SRTP corrispondente, la chiamata non è consentita.
Impostazioni avanzate	Dopo aver selezionato **Massime risorse** o **Applicato** come metodo SRTP, mantenere le altre impostazioni SRTP sui valori predefiniti. Le impostazioni predefinite relativamente a suite di codifica e flag SRTP sono state selezionate in modo da funzionare con tutti i dispositivi SIP e H323 di Avaya. Ad esempio, la maggior parte delle implementazioni Avaya non supporta la codifica RTCP, mentre i telefoni H323 Avaya supportano solo la suite di codifica SHA_80.

4. Fare clic su **OK**.

Collegamenti correlati

Attivazione dell'SRTP di sistema alla pagina 95

Disattivazione di SRTP su un interno o una linea

Procedura

1. Fare clic su **Interno** o **Linea** e selezionare l'interno o la linea secondo necessità.
2. Selezionate il tab **VoIP**.
3. Modificare l'impostazione **Sicurezza supporti** in **Disabilitato**.
4. Fare clic su **OK**.

Passi successivi

Ripetere la procedura per le altre linee o gli altri interni per cui non si intende utilizzare l'SRTP.

Collegamenti correlati

Attivazione dell'SRTP di sistema alla pagina 95

Direct media

Se l'opzione Direct Media è configurata, il sistema tenta la negoziazione Direct Media fra le parti della chiamata. Se l'SRTP è interessato, oltre al controllo dei criteri VoIP corrispondenti (ad esempio il supporto del codec corrispondente), il sistema procede anche al controllo delle impostazioni di Sicurezza supporti, comprese quelle avanzate (flag SRTP e suite di codifica). Eventuali incompatibilità impediranno l'utilizzo di Direct Media da parte delle chiamate.

Le chiamate fra parti impostate su diversi livelli **Sicurezza supporti** (**Disabilitato**, **Massime risorse** o **Applicato**) non utilizzeranno direct media.

Collegamenti correlati

Supporto SRTP alla pagina 95

Capitolo 17: Supporto TLS

Per la versione 10 e successive IP Office, è possibile utilizzare TLS per la connessione dei telefoni 9600. Se abilitata, TLS viene utilizzato per il RAS TCP e la segnalazione di chiamata tra il telefono e il sistema IP Office.

- Supporto nei modelli 9608, 9611, 9621 e 9641.
- Richiede che nel telefono sia in esecuzione il firmware 6.6029 o versioni successive.
- Richiede che il telefono utilizzi una password CRAFT non predefinita.
- È possibile impostare l'utilizzo di TLS da parte del sistema come opzionale o forzato.

Riepilogo della procedura

1. Personalizzare la password Craft per i processi
2. Aggiungere il certificato di sicurezza
3. Abilitare TLS sul sistema IP Office
4. Abilitare TLS nel telefono

Osservazioni supplementari

Per i telefoni che utilizzano TLS:

- La connessione al server dei file HTTPS utilizza la porta 8411. Il server dei file necessita dello stesso certificato.
- In caso di connessione remota tramite SRTP, il telefono utilizza la porta 8443 per backup e ripristino.

Collegamenti correlati

Modifica della password CRAFT alla pagina 98
Aggiunta del certificato di identità alla pagina 99
Download del certificato di identità da un server basato su Linux alla pagina 100
Caricamento di un certificato nell'archivio certificati attendibili del server alla pagina 100
Abilitazione di TLS in IP Office alla pagina 101
Attivazione di TLS sul telefono alla pagina 101
Controllo del funzionamento di TLS alla pagina 102

Modifica della password CRAFT

Informazioni su questa attività

L'impostazione dell'operazione TLS del telefono non può essere modificata abilitata se i telefoni utilizzano la password di processo CRAFT predefinita. È possibile cambiare la password nel modo seguente:

Procedura

1. Se i telefoni stanno scaricando un file `46xxsettings.txt` da un server dei file, effettuare le seguenti operazioni:
   a. Aggiungere una voce **IMPOSTA PROCPSWD** al file `46xxsettings.txt` seguita dalla password da utilizzare.
   b. Riavviare i telefoni per caricare le nuove impostazioni.
2. Se i telefoni utilizzano le impostazioni IP Office generate automaticamente:
   a. Ricevere la configurazione IP Office e individuare l'utente **NoUser**.
   b. Nella scheda **Numeri sorgente**, aggiungere **SET_46xx_PROCPSWD** seguito dalla nuova password.

      Il comando distingue tra maiuscole e minuscole.
   c. Salvare la configurazione e riavviare il sistema.
3. Per visualizzare le impostazioni del file autogenerato:
   a. Aprire il browser e immettere `http://<server_address>/46xxsettings.txt`.
   b. Includere nel file una riga che inizia **IMPOSTA PROCPSWD**, seguita dalla nuova password.

Collegamenti correlati

Supporto TLS alla pagina 98

Aggiunta del certificato di identità

Per impostazione predefinita, viene utilizzato il certificato radice di IP Office. Per i sistemi IP500 V2, si tratta del proprio certificato di protezione autofirmato e non sono richieste ulteriori modifiche. Per i server basati su Linux, è necessario scaricare il certificato autofirmato del server e quindi caricarlo nell'archivio certificati attendibili del servizio IP Office.

Per utilizzare un certificato di terze parti, questo deve essere caricato nell'archivio certificati attendibili di IP Office.

Il telefono riceve l'informazione circa il certificato da utilizzare mediante l'impostazione contenuta nel file `46xxsettings.txt` ricevuto. Vengono utilizzate le impostazioni seguenti:

- `SET TLSSRVRVERIFYID 1`: Questa impostazione indica al telefono di verificare il certificato TLS.
- `SET TRUSTCERTS Root-CA-xxxxxxxx.pem`: Questa impostazione indica il nome del certificato di protezione che deve essere richiesto dal telefono e caricato all'avvio.

  Quando IP Office riceve la richiesta di un certificato, lo ricerca nel proprio archivio certificati attendibili. Se i byte 13-16 della chiave pubblica del CA radice corrispondono alla porzione xxxxxxxx del nome del file nella richiesta, IP Office fornisce il CA radice nella forma di un file autogenerato denominato `Root-CA-xxxxxxxx.pem`.

Per i sistemi che utilizzano file autogenerati, le impostazioni vengono aggiunte automaticamente. Per le altre installazioni, è necessario aggiungere manualmente le impostazioni alla sezione del file 46xxsettings destinata ai telefoni 9608, 9611, 9621 e 9641.

Collegamenti correlati

Supporto TLS alla pagina 98

Download del certificato di identità da un server basato su Linux

Informazioni su questa attività

Procedura

1. Sfogliare https://%3Cserver_address%3E:7071 e accedere ai menu di web control del server.

   In alternativa, accedere ai menu di gestione web del server e quindi selezionare **Visualizzazione piattaforma**.
2. Selezionare la scheda **Impostazioni**, quindi selezionare **Generale**.
3. Individuare la sezione **Certificati** .
4. Nella sezione **Impostazioni autorità di certificazione**, fare clic su **Scarica (codificato PEM)**.

Collegamenti correlati

Supporto TLS alla pagina 98

Caricamento di un certificato nell'archivio certificati attendibili del server

Procedura

1. Avviare IP Office Manager.
2. Selezionare **File** > **Avanzata** > **Impostazioni di sicurezza**
3. Selezionare il server ed effettuare l'accesso.
4. Selezionare **Sistema**.
5. Selezionate il tab **Certificati**.
6. Nella sezione **Archivio certificati affidabili**, fare clic su **Aggiungi**.

Collegamenti correlati

Supporto TLS alla pagina 98

Abilitazione di TLS in IP Office

Informazioni su questa attività

Il sistema IP Office può utilizzare diverse opzioni TLS.

Procedura

1. Utilizzando IP Office Manager, caricare la configurazione del server.
2. Selezionare **Sistema**.
3. Selezionare la scheda **LAN1** o **LAN2**, a seconda dei casi, quindi selezionare la scheda **VoIP**.
4. L'operazione TLS è controllata dal campo **Segnalazione H.323 tramite TLS**. Selezionare la modalità TLS desiderata:
   - **Disabilitato**: Non utilizzare TLS. I telefoni configurati per TLS tornano alla normale connessione TCP.
   - **Preferita**: Utilizzare TLS con i telefoni configurati per TLS, ma consentire anche le normali connessioni TCP da altri telefoni.
   - **Applicato**: Richiede TLS. Le connessioni provenienti dai telefoni non configurati per TLS vengono rifiutate. Se si seleziona questa opzione, **Porta di segnalazione delle chiamate remote** viene fissato a 1300.
5. Fare clic su **OK**.
6. Salvare le modifiche apportate alla configurazione del sistema e consentire il riavvio di quest'ultimo.

Collegamenti correlati

Supporto TLS alla pagina 98

Attivazione di TLS sul telefono

Informazioni su questa attività

L'impostazione TLS per il telefono è accessibile mediante il menu Debug.

Nota:

AAAse si effettua l'upgrade dei telefoni esistenti a un firmware compatibile con TLS, Segnalazione H.323 tramite TLS viene attivata per impostazione predefinita. Tuttavia, nei sistemi non configurati per l'utilizzo di TLS, i telefoni tornano a alla consueta connessione TCP.

Procedura

1. Premere il tasto **DISATTIVA AUDIO** seguito dalla password CRAFT per i processi e dal tasto #.

   Il menu è accessibile nei telefoni mediante la password CRAFT predefinita per i processi. Tuttavia, in tal caso è possibile visualizzare le impostazioni ma non modificarle.

2. Scorrere fino a **DEBUG** e selezionarlo.
3. Scorrere fino a **Segnalazione H.323 tramite TLS**.
4. Modificare l'impostazione secondo necessità.
5. Fare clic su **Salva**.
6. Fare clic su **Esci**.

Risultato

Il telefono viene riavviato e utilizza le nuove impostazioni.

Collegamenti correlati

Supporto TLS alla pagina 98

Controllo del funzionamento di TLS

È possibile controllare e confermare l'utilizzo di TLS come indicato di seguito.

- System Status Application: i dettagli **Interno** indicano che **Protocollo di livello** viene utilizzato dalla connessione all'interno. **TLS** viene visualizzato quando si utilizza TLS.
- Monitor di sistema: all'interno del monitor, selezionare **Stato** > **Stato telefono H323**. La **Trasporto**colonna mostra **TLS** gli interni che utilizzano TLS per la connessione.

  All'interno delle tracce di Monitor, i record relativi a Tx e Rx RAS H323 indicano l'eventuale utilizzo di TLS. In modo analogo, i record CS e RAS H323 indicano l'utilizzo della porta 1300.

Collegamenti correlati

Supporto TLS alla pagina 98

Parte 5: Varie

Capitolo 18: Opzioni di amministrazione statica

Dopo l'installazione è possibile modificare diverse impostazioni tramite il telefono. Queste procedure devono essere utilizzate solo se si utilizza l'installazione dell'indirizzo statico. Non seguire queste procedure in caso di utilizzo di DHCP, a meno che non si tenti di riassegnare un telefono precedentemente installato in modo statico.

Per impostare i parametri di tutti i telefoni IP H.323 in un sistema è possibile modificare il file di script `46xxsettings.txt`. I valori assegnati tramite l'amministrazione statica hanno tuttavia la precedenza sui valori impostati tramite il file 46xxsettings.txt, ma rimarranno attivi per il telefono IP fino al download di un nuovo file di avvio.

Collegamenti correlati

Utilizzo di opzioni di amministrazione statica alla pagina 104
Password per il processo di amministrazione alla pagina 106
Attivazione dell'interfaccia hub alla pagina 106
Visualizzare i dettagli del telefono alla pagina 108
Procedura di autotest per i telefoni serie 1600 alla pagina 110
Procedura di autotest per i telefoni serie 9600 alla pagina 110
Ripristino di un telefono alla pagina 111
Formattazione di un telefono alla pagina 112
SSON (Site Specific Option Number) alla pagina 113

Utilizzo di opzioni di amministrazione statica

Il metodo utilizzato per accedere all'amministrazione statica dipende dal tipo di telefono. È possibile accedere a molte funzioni di amministrazione statica attraverso una sequenza di tasti, che inizia premendo il tasto **DISATTIVA AUDIO** o **ATTESA**. Nelle versioni recenti del firmware è stata data preferenza all'utilizzo del tasto **DISATTIVA AUDIO** e alcuni telefoni, come quelli della serie 1600, supportano solo il tasto **DISATTIVA AUDIO**.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104
Immissione delle opzioni di amministrazione nei telefoni serie 1600 alla pagina 105
Immissione delle opzioni di amministrazione nei telefoni serie 9600 alla pagina 105

Immissione delle opzioni di amministrazione nei telefoni serie 1600

Informazioni su questa attività

Questa sezione illustra come inserire i dati per le opzioni amministrative.

Procedura

1. Se il telefono è inattivo, premere **DISATTIVA AUDIO**.

   Dopo aver premuto **DISATTIVA AUDIO**, se non si premere un pulsante valido entro 6 secondi dal precedente, le cifre raccolte vengono rimosse e il telefono torna allo stato di inattività.
2. Comporre la password per il processo di amministrazione
3. Comporre le cifre per il comando richiesto, seguite da #.
   - I tentativi di inserimento di dati errati vengono rifiutati e viene emesso un segnale di errore dal telefono.
   - Se viene inserito un tasto numerico come valore o in un campo che prevede un indirizzo IP o una maschera di sottorete dopo aver inserito soltanto uno zero, la nuova cifra sostituirà lo zero.
   - Per procedere al passaggio successivo, premere #.

Collegamenti correlati

Utilizzo di opzioni di amministrazione statica alla pagina 104

Immissione delle opzioni di amministrazione nei telefoni serie 9600

Informazioni su questa attività

È possibile accedere alle procedure amministrative per i telefoni di serie 9600 solo riavviando il telefono.

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu fino all'azione richiesta e selezionarla.

   Una volta completata la procedura selezionata, il telefono tornerà al menu delle procedure.
3. Una volta completate tutte le procedure richieste, premere **Esci**.

Risultato

Il telefono viene riavviato con nuove impostazioni.

Collegamenti correlati

Utilizzo di opzioni di amministrazione statica alla pagina 104

Password per il processo di amministrazione

Informazioni su questa attività

I processi amministrativi del telefono sono protetti da un'apposita password, nota anche come password CRAFT. È possibile cambiare la password predefinita specificando il nuovo valore nel file `46xxsettings.txt`.

Procedura

1. Se i telefoni stanno scaricando un file `46xxsettings.txt` da un server dei file, effettuare le seguenti operazioni:
   a. Aggiungere una voce **IMPOSTA PROCPSWD** al file `46xxsettings.txt` seguita dalla password da utilizzare.
   b. Riavviare i telefoni per caricare le nuove impostazioni.
2. Se i telefoni utilizzano le impostazioni IP Office generate automaticamente:
   a. Ricevere la configurazione IP Office e individuare l'utente **NoUser**.
   b. Nella scheda **Numeri sorgente**, aggiungere **SET_46xx_PROCPSWD** seguito dalla nuova password.

      Il comando distingue tra maiuscole e minuscole.
   c. Salvare la configurazione e riavviare il sistema.
3. Per visualizzare le impostazioni del file autogenerato:
   a. Aprire il browser e immettere `http://<server_address>/46xxsettings.txt`.
   b. Includere nel file una riga che inizia **IMPOSTA PROCPSWD**, seguita dalla nuova password.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104

Attivazione dell'interfaccia hub

L'interfaccia hub si trova su molti telefoni IP Avaya che possono essere utilizzati per la connessione PC utente. L'interfaccia hub è attivata per impostazione predefinita.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104
Attivazione dell'interfaccia hub per i telefoni serie 1600 alla pagina 107
Attivazione dell'interfaccia hub per la serie 9600 alla pagina 107

Attivazione dell'interfaccia hub per i telefoni serie 1600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> INT #` o `MUTE <password> 468 #`.

   Le impostazioni per le porte dei telefoni vengono mostrate in sequenza. Le opzioni variano a seconda del modello di telefono.

   - `PHY2=`

     La presa LAN del collegamento al PC indicata sul telefono con . Premere 1 o 0 rispettivamente per attivare o disattivare l'interfaccia hub. Per continuare, premere #.

   - `IR=`

     La porta a infrarossi (IR) collocata sulla parte anteriore di alcuni telefoni IP H.323. Premere 1 o 0 rispettivamente per attivare o disattivare l'interfaccia hub. Per continuare, premere #.

2. Premere # per salvare i nuovi valori.

Risultato

Viene visualizzato `salvataggio nuovi valori in corso`, quindi il telefono torna al normale funzionamento.

Collegamenti correlati

Attivazione dell'interfaccia hub alla pagina 106

Attivazione dell'interfaccia hub per la serie 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu fino a **INTERNO**.
3. Selezionare la porta che si desidera regolare. Le opzioni sono **Ethernet** e **PC Ethernet**.
4. Utilizzare i pulsanti < e > per scorrere le varie impostazioni possibili per la porta.

   L'opzione aggiuntiva **Disabilitato** è disponibile per la porta Ethernet del PC.

5. Premere **Salva**.
6. Selezionare un'altra procedura o premere **Esci** per riavviare il telefono.

Collegamenti correlati

Attivazione dell'interfaccia hub alla pagina 106

Visualizzare i dettagli del telefono

È possibile visualizzare una serie di dettagli del telefono. e di amministrazione locale utilizzabili anche per rivedere le impostazioni.

Collegamenti correlati

[Opzioni di amministrazione statica](#) alla pagina 104
[Visualizzazione dei dettagli dei telefoni serie 1600](#) alla pagina 108
[Visualizzazione dei dettagli dei telefoni serie 9600](#) alla pagina 109

Visualizzazione dei dettagli dei telefoni serie 1600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE CRAFT VIEW #` o `MUTE 27238 8439 #`.
2. Per visualizzare i dettagli, premere il tasto * in qualsiasi momento durante la visualizzazione. Vengono visualizzate le seguenti impostazioni:

Valore	Descrizione
Modello	Mostra il numero del modello del telefono, ad esempio 4624D02A.
Mercato	Viene visualizzato 1 per l'export e 0 per il mercato nazionale (USA). Alcuni tipi di telefoni non visualizzano questa informazione.
Numero di telefono	Mostra il numero di serie del telefono.
SN PWB	Mostra il **numero di serie sul circuito stampato (PWB, Printed Wiring Board)** del telefono.
Comcode PWB	Mostra il comcode del circuito stampato (PWB, Printed Wiring Board).
Indirizzo MAC	Mostra l'indirizzo MAC del telefono in coppie esadecimali.
Etichettatura L2	Indica se il tagging L2 è **su**, **disattivato** o impostato su **auto**.
ID VLAN	Utilizzato per il telefono. Il valore predefinito è 0.
Indirizzo IP	L'indirizzo IP assegnato al telefono.
Subnet mask	La Subnet Mask assegnata al telefono.
Router	L'indirizzo router assegnato al telefono.
Server del file	L'indirizzo del file server assegnato al telefono.
Server di chiamata	L'indirizzo del gatekeeper H.323 del telefono.
802.1X	L'impostazione corrente per il funzionamento di 802.1X, se in uso.
Gruppo	Mostra il valore di gruppo impostato sul telefono. I valori di gruppo consentono di controllare quali opzioni (firmware e impostazioni) vengono scaricate dal telefono.
Protocollo	Visualizza **Predefinito**.
nomefile1	Mostra il nome del file applicazione del telefono nella memoria del telefono. Questi valori sono all'interno del file di avvio caricato e non corrispondono al nome effettivo del file.

La tabella continua…

Valore	Descrizione
10MBps Ethernet **Ethernet a 100Mbps**	Mostra la velocità della connessione LAN individuata.
nomefile2	Mostra il nome e il livello del file di avvio. Questi valori sono all'interno del file di avvio caricato e non corrispondono al nome effettivo del file.

3. Per terminare la procedura e ripristinare l'interfaccia utente sullo stato precedente, premere il tasto #.
4. Per visualizzare il valore seguente, premere *.

Collegamenti correlati

Visualizzare i dettagli del telefono alla pagina 108

Visualizzazione dei dettagli dei telefoni serie 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu fino a **VISUALIZZA** e avviare la procedura.

Valore	Descrizione
Modello	Mostra il numero di modello del telefono, ad esempio 4624D02A.
Numero di telefono	Mostra il numero di serie del telefono.
SN PWB	Mostra il **numero di serie sul circuito stampato (PWB, Printed Wiring Board)** del telefono.
Comcode PWB	Mostra il comcode del circuito stampato (PWB, Printed Wiring Board).
MAC	Mostra l'indirizzo MAC del telefono in coppie esadecimali.
Gruppo	Mostra il valore del gruppo impostato sul telefono. I valori di gruppo consentono di controllare quali opzioni (firmware e impostazioni) vengono scaricate dal telefono.
Protocollo	Visualizza **Predefinito**.
File applicazione	Mostra il nome del file applicazione del telefono nella memoria del telefono. Questi valori sono all'interno del file di avvio caricato e non corrispondono al nome effettivo del file.
Ethernet	Mostra la velocità della connessione LAN individuata.
File di avvio	Mostra il nome e il livello del file di avvio. Questi valori sono all'interno del file di avvio caricato e non corrispondono al nome effettivo del file.
Server proxy	Mostra i dettagli del server proxy selezionato.
File lingua vocale	Il nome del file di lingua in uso nel telefono. Il campo è vuoto in caso di utilizzo della lingua predefinita (inglese).

3. Premere **Indietro**.
4. Selezionare un'altra procedura o premere **Esci** per riavviare il telefono.

Collegamenti correlati

Visualizzare i dettagli del telefono alla pagina 108

Procedura di autotest per i telefoni serie 1600

Procedura

1. Per avviare la procedura di autotest del telefono IP, premere `MUTE <password> TEST #` o `MUTE <password> 8378 #`.

   Il telefono esegue le operazioni descritte di seguito:

   - Ogni colonna di LED dei tasti programmabili si accende per mezzo secondo da sinistra a destra per tutto il telefono secondo un ciclo ripetitivo. Si accendono in sequenza anche il LED Altoparlante/Muto e il LED del messaggio in attesa.
   - Tutti i tasti (ad eccezione di #) producono un clic se premuti.
   - Sui telefoni con display, viene visualizzato `Autotest #=fine` per un secondo dopo l'avvio dell'autotest. Viene quindi visualizzato un carattere di blocco (con tutti i pixel attivati) in tutte le posizioni dei caratteri sul display per cinque secondi. La visualizzazione del carattere di blocco viene utilizzata per individuare i pixel non visualizzati correttamente.
   - Se l'autotest viene superato:

     ```
     Self test passed
     #=end
     ```

   - Se l'autotest non viene superato:

     ```
     Self test failed
     #=end
     ```

2. Per terminare l'autotest, premere il tasto #.

Risultato

Il telefono torna al normale funzionamento.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104

Procedura di autotest per i telefoni serie 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu fino a **Test**.
3. Premere nuovamente **Test** per confermare l'azione.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104

Ripristino di un telefono

Il ripristino di un telefono comporta il ripristino di tutti i valori e della maggior parte dei valori di inizializzazione del sistema. La procedura non incide sui dati e sulle impostazioni specificati dall'utente (esempio Dati dei contatti, Impostazioni di opzioni, password o interno di accesso e così via). Per rimuovere tutti questi dati, fare riferimento a Formattazione di un telefono alla pagina 112.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104
Ripristino del telefono serie 1600 alla pagina 111
Ripristino del telefono serie 9600 alla pagina 111

Ripristino del telefono serie 1600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere la seguente sequenza `MUTE <password> RESET #`

   `MUTE <password> 73738 #`

   Avvertenza:

   Non appena si preme il tasto #, tutte le informazioni statiche saranno cancellate senza possibilità di recupero dei dati.

2. Per continuare, premere #.

   Mentre i valori di sistema vengono ripristinati ai valori predefiniti, viene visualizzato il messaggio Reset valori.

   Una volta ripristinati i valori del sistema viene visualizzato `Riavviare il telefono?`

3. Per terminare la procedura senza riavviare il telefono, premere *.
4. Per riavviare il telefono, premere #.

   La parte restante della procedura dipende poi dallo stato dei file di avvio e dell'applicazione. Consultare Scenari di riavvio alla pagina 115.

Collegamenti correlati

Ripristino di un telefono alla pagina 111

Ripristino del telefono serie 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu e selezionare **Reimposta valori**.
3. Premere **Reimposta** per confermare l'azione.

Risultato

Le impostazioni utente del telefono verranno reimpostate al riavvio del telefono.

Collegamenti correlati

Ripristino di un telefono alla pagina 111

Formattazione di un telefono

Il ripristino di tutti i valori di inizializzazione del sistema sulle impostazioni predefinite e l'eliminazione di tutti i dati specifici dell'utente sono operazioni destinate essenzialmente alla riparazione e all'utilizzo del telefono da parte di un nuovo utente. Il telefono viene praticamente riportato al suo stato originale appena acquistato, ma conserverà i file firmware già scaricati.

Nota:

è possibile impostare alcuni parametri, come i clic sui pulsanti, i toni di errore e le suonerie personalizzate, per un utente specifico tramite MENU. Queste impostazioni utente verranno ripristinate al momento della registrazione dell'utente al telefono, in quanto i parametri sono configurati in IP Office. Tutte le altre impostazioni (ad esempio Dati dei contatti, Impostazioni di opzioni e così via) sono cancellate dal telefono.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104
Cancellazione dei telefoni serie 1600 alla pagina 112
Cancellazione dei telefoni serie 9600 alla pagina 113

Cancellazione dei telefoni serie 1600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere la seguente sequenza `MUTE <password> CLEAR #`.

   `MUTE <password> 25327 #`

2. Per continuare, premere #.

   Avvertenza:

   Non appena si preme il tasto #, tutte le informazioni statiche saranno cancellate senza possibilità di recupero dei dati.

   Mentre i valori di sistema vengono ripristinati sui valori predefiniti, viene visualizzato il messaggio `Cancellazione valori in corso`.

Risultato

Una volta cancellati tutti i valori, il telefono viene riavviato come se fosse nuovo.

Collegamenti correlati

Formattazione di un telefono alla pagina 112

Cancellazione dei telefoni serie 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2.
3. Scorrere il menu e selezionare **Cancella**.
4. Premere nuovamente **Cancella** per confermare l'azione.

Risultato

Le impostazioni del telefono vengono cancellate e il telefono viene riavviato.

Collegamenti correlati

Formattazione di un telefono alla pagina 112

SSON (Site Specific Option Number)

Il numero opzione specifico per sito (SSON) è utilizzato dai telefoni IP per richiedere informazioni da un server DHCP utilizzato specificatamente per questi telefoni e non per altri dispositivi IP supportati dal server DHCP. Questo numero deve corrispondere a una "opzione" numerata allo stesso modo, impostata sul server DHCP che definisce le varie impostazioni richieste dal telefono.

Il numero SSON predefinito utilizzato dai telefoni delle serie 1600 e 9600 Avaya è 242. Per i telefoni supportati da DHCP IP Office, il numero SSON utilizzato dal telefono deve corrispondere a uno dei numeri di opzione specifici del sito impostati nella configurazione IP Office

Avvertenza:

Non eseguire questa operazione se si utilizzano indirizzi statici. Eseguire questa operazione solo se si utilizzano indirizzi DHCP e se il numero dell'opzione DHCP è stato modificato rispetto a quello predefinito.

Collegamenti correlati

Opzioni di amministrazione statica alla pagina 104
SSON nei telefoni serie 1600 alla pagina 113
SSON nella serie di telefoni 9600 alla pagina 114

SSON nei telefoni serie 1600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> SSON #` o `MUTE <password> 7766 #`

   SSON= viene visualizzato seguito dal valore corrente.

2. Inserire la nuova impostazione. Deve essere un numero compreso tra 128 E 255.
3. Per annullare la procedura, premere il tasto * oppure premere il tasto # per salvare il nuovo valore.

Collegamenti correlati

SSON (Site Specific Option Number) alla pagina 113

SSON nella serie di telefoni 9600

Procedura

1. Mentre il telefono è agganciato e inattivo, premere `MUTE <password> #`.
2. Scorrere il menu fino a **SSON** e avviare la procedura.
3. Immettere il nuovo numero SSON che il telefono deve utilizzare al successivo riavvio.
4. Premere **Salva**.
5. Selezionare un'altra procedura o premere **Esci** per riavviare il telefono.

Collegamenti correlati

SSON (Site Specific Option Number) alla pagina 113

Capitolo 19: Scenari di riavvio

La sequenza del processo di riavvio varia a seconda della versione del file di avvio del telefono già scaricato nel telefono e sul server dei file. Questa appendice illustra i diversi scenari possibili.

Tutte le procedure di avvio descritte di seguito comprendono le stesse procedure iniziali, in quanto il telefono negozia con il server DHCP e il file server.

1. Dopo aver collegato l'alimentazione, il telefono visualizza `Riavvio` seguito da `Inizializzazione`
2. Quando il file applicazione (se presente) o il codice di avvio viene decompresso nella RAM, viene visualizzato Caricamento in corso. Questa operazione richiede alcuni minuti durante i quali sulla seconda riga viene visualizzata una sequenza di asterischi, punti e asterischi per indicare che il caricamento è in corso.
3. Quando il controllo viene passato al codice nella RAM, viene visualizzato `Avvio in corso`.
4. Il telefono individua e visualizza la velocità dell'interfaccia Ethernet in Mbps (cioè 10 o 100). Il messaggio No Ethernet indica che è impossibile determinare la velocità dell'interfaccia LAN. La velocità Ethernet indicata è la velocità dell'interfaccia LAN per il telefono e qualsiasi PC collegato.
5. Mentre il telefono ottiene l'indirizzo IP e altre informazioni dal server DHCP della LAN viene visualizzato DHCP. Il numero di secondi trascorsi viene incrementato fino al completamento del DHCP.
   - Se il telefono è stato configurato con un indirizzo statico (premendo il tasto * quando viene visualizzato DHCP), ignorerà il DHCP e utilizzerà le impostazioni dell'indirizzo statico inserite.
   - Si noti che ogni volta che si carica un nuovo file di avvio, le informazioni sull'indirizzo statico verranno cancellate.
6. Una volta completata la richiesta DHCP, il telefono richiede i file dal file server indicato nella risposta DHCP. Il primo file richiesto contiene i dettagli degli altri file che devono essere caricati dal telefono. Il telefono effettua in primo luogo la richiesta dei file mediante HTTPS. In caso di esito negativo, effettua la stessa richiesta mediante HTTP. In caso di esito negativo, effettua una richiesta finale mediante TFTP. Se tutte le richieste avranno esito negativo, il telefono utilizza la versione corrente del file presente nella memoria.
7. Dopo aver caricato lo script di aggiornamento, la sequenza dipenderà dallo stato dei file presenti nella memoria del telefono, rispetto a quelli elencati nel file di script di aggiornamento.

Collegamenti correlati

[Aggiornamento del file di avvio](#) alla pagina 116
[Nessun file applicazione o aggiornamento del file applicazione necessario](#) alla pagina 116
[File di avvio e file applicazione corretti già caricati](#) alla pagina 117

Aggiornamento del file di avvio

Dopo aver elaborato il file di script di upgrade, il software stabilisce che il nome del file del codice di avvio nel telefono non corrisponde a quello nello script di upgrade. Il nome del nuovo file da caricare viene specificato dallo script.

1. Il nome del file e il numero di kilobyte caricati vengono visualizzati sul telefono.
2. Durante l'archiviazione del file di avvio nella memoria flash del telefono, su quest'ultimo viene visualizzato `Saving to flash`. Viene visualizzata la percentuale del file memorizzato e il numero di secondi trascorsi. Normalmente questa operazione impiega più tempo dello scaricamento del file.
3. Durante la preparazione al riavvio tramite il nuovo file di avvio, sul telefono viene visualizzato `Riavvio in corso`.
4. Sul telefono viene visualizzato `Inizializzazione in corso`.
5. Durante la decompressione del nuovo file di avvio nella RAM, sul telefono viene visualizzato `Caricamento in corso`. Questa operazione richiede alcuni minuti durante i quali sulla seconda riga viene visualizzata una sequenza di asterischi, punti e asterischi per indicare che il caricamento è in corso.
6. Quando il controllo viene passato al software appena caricato, sul telefono viene visualizzato `Avvio in corso`.
7. Durante la cancellazione della memoria flash per la preparazione alla scrittura del codice, sul telefono viene visualizzato `Cancellazione in corso`. Viene visualizzata la percentuale di memoria cancellata e il numero di secondi trascorsi.
8. Durante la riscrittura del codice di avvio viene visualizzato Aggiornamento. Nel telefono verrà inoltre visualizzata la percentuale di codice di avvio riscritto e il numero di secondi trascorsi.
9. Se il nuovo codice di avvio viene scritto correttamente nella memoria flash, il telefono viene ripristinato in modo da rendere possibile il controllo dello stato dei file applicazione del telefono.

Collegamenti correlati

Scenari di riavvio alla pagina 115

Nessun file applicazione o aggiornamento del file applicazione necessario

Questa procedura è valida per i normali aggiornamenti del file applicazione. Dopo aver elaborato lo script di aggiornamento, il software determina che il nome del file di avvio nel telefono è della corretta versione. In seguito determina che il nome del file applicazione non corrisponde a quello memorizzato nel telefono.

1. Il nome del file necessario viene visualizzato sul telefono mentre viene scaricato dal server TFTP. Viene inoltre visualizzato il numero di kilobyte scaricati.
2. Viene visualizzato `Salvataggio nella memoria flash in corso`. Nel telefono vengono inoltre visualizzati la percentuale del file archiviato e il numero di secondi

trascorsi. Normalmente questa operazione impiega più tempo dello scaricamento del file.

3. Il telefono viene reimpostato in modo da rendere possibile l'esecuzione del file applicazione specifico per il sistema.

Collegamenti correlati

Scenari di riavvio alla pagina 115

File di avvio e file applicazione corretti già caricati

Questa procedura è valida nella maggior parte dei normali riavvii. Dopo aver elaborato lo script di aggiornamento, il software determina che il nome del file di avvio nel telefono e quello del file applicazione del telefono corrispondono a quelli specificati nello script di aggiornamento.

1. Viene avviata la registrazione con lo switch del sistema specifico. Il telefono richiede il numero di interno e la password da utilizzare.
   - Per impostazione predefinita, il telefono visualizza l'ultimo numero di interno utilizzato. Per accettare, premere il tasto #.
   - Salvo il caso in cui l'utente modifichi il numero di interno, non viene effettuata alcuna verifica di password mentre viene visualizzata la richiesta di password.
   - La password viene verificata in base all'interno **Password telefonica** memorizzato in IP Office Manager. Se non è stato impostato una **Password telefonica**, il sistema effettua anche il controllo del codice di accesso dell'utente corrispondente. I sistemi precedenti a IP Office versione 9.0 utilizzano solo il **Codice accesso** dell'utente corrispondente.
2. Al termine della registrazione sarà disponibile un segnale di linea sul telefono se quest'ultimo è stato abilitato per ottenere una licenza interno o una sottoscrizione utente.

Collegamenti correlati

Scenari di riavvio alla pagina 115

Capitolo 20: Risorse

Documentazione

Ricerca di documenti sul sito Web dell'assistenza Avaya

Procedura

1. Accedere a https://support.avaya.com.
2. Nella parte superiore della schermata, digitare il nome utente e la password e fare clic su **Login**.
3. Fare clic su **Support by Product** > **Documents**.
4. In **Enter your Product Here** digitare il nome del prodotto e selezionarlo dall'elenco.
5. In **Choose Release** selezionare il numero di versione appropriato.

   Il campo **Choose Release** non è disponibile se è presente una sola versione del prodotto.
6. Nel filtro **Content Type**, fare clic su un tipo di documento o fare clic su **Select All** per visualizzare un elenco di tutti i documenti disponibili.

   Ad esempio, per i Manuali dell'utente fare clic su **User Guides** nel filtro **Content Type**. L'elenco mostra solo i documenti della categoria selezionata.
7. Fare clic su **Enter**.

Formazione

Visualizzazione di Avaya Mentor videos

Avaya Mentor videos offre informazioni tecniche su come installare, configurare e risolvere i problemi dei prodotti Avaya.

Informazioni su questa attività

I video sono disponibili sul sito Web di assistenza Avaya, elencati sotto il tipo di documento video, e sul canale di YouTube gestito da Avaya.

- Per trovare i video sul sito Web dell'assistenza Avaya, accedere all'indirizzo https://support.avaya.com/ ed effettuare una delle operazioni seguenti:
  - In **Search**, digitare `Video Avaya Mentor`, fare clic su **Cancella tutto** e selezionare **Video** in **Content Type**.
  - In **Search** digitare il nome del prodotto. Sulla pagina **Search Results**, fare clic su **Cancella tutto** e selezionare **Video** in **Content Type**.

    Il tipo di contenuto di **Video** viene visualizzato solo quando sono disponibili video per quel prodotto.

  Nel riquadro a destra, viene visualizzato un elenco dei video disponibili.
- Per trovare i video di Avaya Mentor su YouTube, visitare il sito Web www.youtube.com/AvayaMentor ed effettuare una delle operazioni seguenti:
  - Immettere una o più parole chiave nel campo **Cerca nel canale** per trovare un prodotto o un argomento specifico.
  - Scorrere **Playlists** verso il basso e fare clic sul nome di un argomento per visualizzare l'elenco dei video disponibili per esso. Ad esempio, "Contact Centers".

  Nota:

  Non sono disponibili video per tutti i prodotti.

Assistenza

Visitare il sito Web dell'assistenza Avaya all'indirizzo https://support.avaya.com per gli articoli illustrativi, le comunicazioni di prodotti e i documenti più aggiornati. È anche possibile cercare note di rilascio, scaricamenti e risoluzioni a problemi. Utilizzare il sistema di richiesta di assistenza online per creare una richiesta di assistenza tecnica. Chattare con agenti collegati per ricevere risposte alle domande o per chiedere di essere connessi a un team di assistenza se un problema richiede un intervento tecnico più approfondito.

Collegamenti correlati

Utilizzo della Knowledge Base Avaya InSite alla pagina 119

Utilizzo della Knowledge Base Avaya InSite

La Knowledge Base di Avaya InSite è un motore di ricerca basato sul Web che fornisce:

- Procedure di risoluzione dei problemi aggiornate e suggerimenti tecnici
- Informazioni sui service pack
- Accesso alla documentazione tecnica e destinata al cliente
- Informazioni sui programmi di formazione e certificazione

- Collegamenti ad altre informazioni pertinenti

Se l'utente è un partner Avaya autorizzato o un cliente Avaya attuale con un contratto di assistenza, è possibile accedere alla knowledge base senza costi aggiuntivi. È necessario disporre di un account di accesso e di un numero di acquirente valido.

Utilizzare la knowledge base Avaya InSite per trovare possibili soluzioni ai problemi.

1. Accedere a http://www.avaya.com/support.
2. Accedere al sito Web Avaya utilizzando un ID utente e una password Avaya validi.

   Il sistema visualizza la pagina **Avaya Support**.
3. Fare clic su **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, immettere il prodotto e premere `Invio`.
5. Selezionare il prodotto dall'elenco e selezionare una versione.
6. Fare clic sulla scheda **Technical Solutions** per visualizzare gli articoli.
7. Selezionare gli articoli pertinenti.

Collegamenti correlati

Assistenza alla pagina 119

Indice

H

I

K

L

M

N

O

P

Q

R

S

T

U

V