Guida per il provisioning dei telefoni multipiattaforma Cisco IP Phone serie 6800

Prima pubblicazione: 2017-11-22

Ultima modifica: 2019-08-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

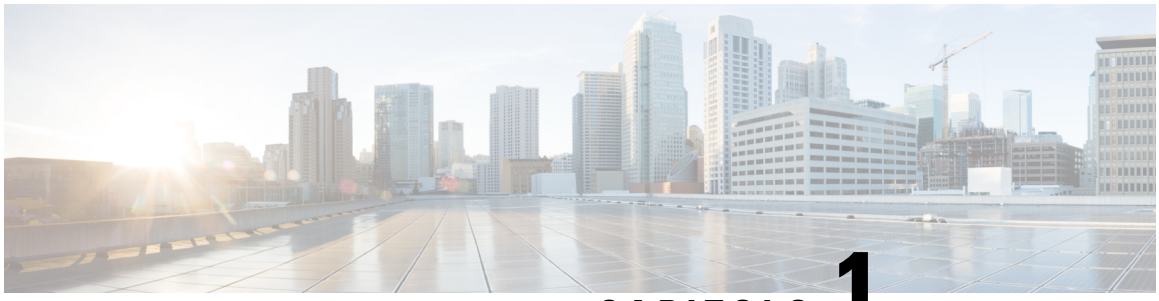
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

SOMMARIO



CAPITOLO 1

Distribuzione e provisioning

Novità e modifiche

Novità e modifiche per la versione del firmware 11.2(4)

Revisione	Sezioni nuove e modificate
Aggiunti parametri per le impostazioni Wi-Fi	Esempio di formato Open XML, a pagina 81

Novità e modifiche per la versione del firmware 11.2(3)SR1

Le sezioni seguenti sono nuove o aggiornate per supportare Telefoni multipiattaforma Cisco IP Phone serie 6800.

Revisioni	Sezioni nuove e modificate
Aggiunto un nuovo argomento per spiegare l'onboardig tramite codice di attivazione.	Onboarding del telefono con il codice di attivazione , a pagina 11

Novità e modifiche per la versione del firmware 11.2(3)

Le sezioni seguenti sono nuove o aggiornate per supportare Telefoni multipiattaforma Cisco IP Phone serie 6800.

Revisioni	Sezioni nuove e modificate
Aggiunto un argomento concettuale per la crittografia di un profilo Open	Crittografia di profilo Open, a pagina 20
Aggiunto un nuovo argomento per introdurre la crittografia dei contenuti HTTP basata su RFC 8188	Crittografia dei contenuti HTTP basata su RFC 8188, a pagina 24
Aggiornata con informazioni dettagliate sulla crittografia basata su RFC 8188.	Formati dei profili di configurazione, a pagina 15 Provisioning su HTTP, a pagina 45
Aggiornate le informazioni introduttive per la crittografia del profilo Open.	Crittografia AES-256-CBC, a pagina 21
Aggiornata la descrizione dell'opzione**`--key`** e aggiunta una nota sulla crittografia basata su RFC 8188.	key, a pagina 25 Parametri di configurazione profili, a pagina 69
Aggiornati gli esempi di formato Open XML con nuovi parametri e le opzioni disponibili	Esempio di formato Open XML, a pagina 81

Novità e modifiche per la versione del firmware 11.2(1)

Revisioni	Sezioni nuove o modificate
Aggiornato l'argomento con un riferimento al confronto dei parametri XML e TR69	Provisioning di TR69, a pagina 4
Aggiunto un nuovo argomento per supportare la funzionalità di intestazione privacy	Impostazione dell'intestazione privacy del telefono, a pagina 67
Aggiunto un nuovo argomento per supportare la condivisione del firmware	Condivisione del firmware, a pagina 12
Aggiornato questo argomento con i metodi di crittografia	Come ottenere un certificato del server firmato, a pagina 48
Aggiornato questo argomento per ignorare la schermata **Imposta password**	Controllo dell'accesso di configurazione, a pagina 9
Aggiunto un nuovo argomento per ignorare la schermata **Imposta Password**	Come ignorare la schermata Imposta password, a pagina 13

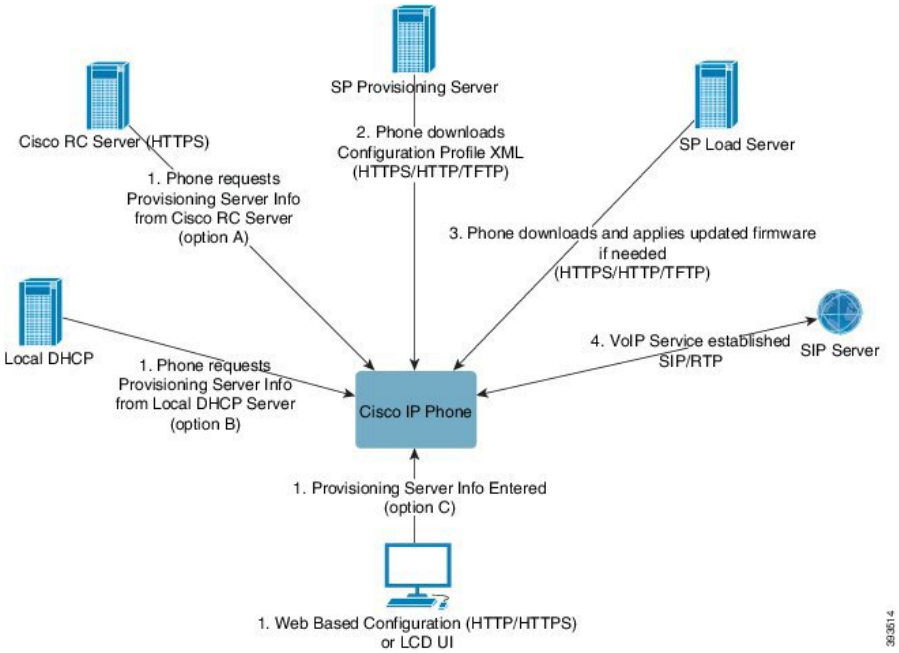
Panoramica del provisioning

I telefoni Cisco IP Phone sono destinati a distribuzioni con volumi elevati da provider di servizi VoIP (Voice-over-IP) a clienti residenziali, attività commerciali e aziende. Pertanto, il provisioning del telefono tramite gestione e configurazione remote garantisce il corretto funzionamento del telefono presso la sede del cliente.

Cisco supporta la configurazione continua e personalizzata delle funzioni del telefono nel seguente modo:

- Controllo remoto affidabile del telefono.
- Crittografia della comunicazione che consente di controllare il telefono.
- Associazione di account del telefono semplificata.

Il provisioning dei telefoni può essere eseguito mediante download dei profili di configurazione o aggiornamento del firmware da un server remoto. I download possono essere eseguiti quando i telefoni sono connessi a una rete, quando vengono accesi e a intervalli impostati. Il provisioning in genere fa parte di distribuzioni VoIP con volumi elevati ed è comune ai provider di servizi. I profili di configurazione o il firmware aggiornato vengono trasferiti nel dispositivo tramite TFTP, HTTP o HTTPS.



A un livello elevato, la procedura di provisioning è la seguente:

1. Se il telefono non è configurato, le informazioni sul server di provisioning vengono applicate al telefono utilizzando una delle seguenti opzioni:
   - **A**–Download dal server di personalizzazione remota (RC) di Cisco Enablement Data Orchestration System (EDOS) utilizzando HTTPS.
   - **B**–Query dal server DHCP locale.
   - **C**–Inserimento tramite l'utilità di configurazione basata sul Web del telefono Cisco o tramite l'interfaccia utente del telefono.
2. Il telefono scarica le informazioni sul server di provisioning e applica il file XML di configurazione tramite HTTPS, HTTP o TFTP.
3. Il telefono scarica e applica il firmware aggiornato, se necessario, tramite HTTPS, HTTP o TFTP.
4. Il servizio VoIP viene definito tramite la configurazione e il firmware specificati.

Il provider di servizi VoIP intende distribuire molti telefoni a clienti residenziali e piccole aziende. Negli ambienti di aziende medio-grandi, i telefoni possono servire come nodi terminali. Questi dispositivi, connessi tramite router e firewall presso la sede del cliente, vengono distribuiti su larga scala su Internet.

Il telefono può essere utilizzato come un interno remoto delle attrezzature di back-end del provider di servizi. Configurazione e gestione remote assicurano il corretto funzionamento del telefono presso la sede del cliente.

Provisioning di TR69

Il Cisco IP Phone consente all'amministratore di configurare i parametri TR69 tramite l'interfaccia utente Web. Per informazioni relative ai parametri, incluso un confronto tra i parametri XML e TR69, consultare la Guida all'amministrazione per la serie del telefono corrispondente.

I telefoni supportano l'individuazione di ACS (Auto Configuration Server) da DHCP opzione 43, 60 e 125.

- Opzione 43: informazioni specifiche del fornitore per l'URL ACS.
- Opzione 60: identificatore della classe del fornitore per consentire al telefono di identificarsi con `dslforum.org` su ACS
- Opzione 125: informazioni specifiche del fornitore per associazione gateway.

Metodi RPC

Metodi RPC supportati

I telefoni supportano solo una serie limitata di metodi RPC (Remote Procedure Call) come segue:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: metodo Download RPC, i tipi di file supportati sono:
    - Immagine di aggiornamento del firmware
    - File di configurazione del fornitore

    - File CA (Certificate Authority) personalizzato
- Trasferimento completo

Tipi di eventi supportati

I telefoni supportano i tipi di evento in base alle funzionalità e ai metodi supportati. Sono supportati solo i seguenti tipi di eventi:

- Bootstrap
- Boot
- modifica del valore
- richiesta di connessione
- Periodica
- Trasferimento completo
- Download M
- Reboot M

Crittografia delle comunicazioni

I parametri di configurazione che vengono comunicati al dispositivo possono contenere codici di autorizzazione o altre informazioni che proteggono il sistema da accesso non autorizzato. È nell'interesse del provider di servizi impedire attività del cliente non autorizzate. È nell'interesse del cliente evitare l'utilizzo dell'account in modo non autorizzato. Il provider di servizi può crittografare la comunicazione dei profili di configurazione tra il server di provisioning e il dispositivo, oltre a limitare l'accesso al server Web di amministrazione.

Comportamento del telefono durante le ore di congestione della rete

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

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

Distribuzione

I Cisco IP Phone forniscono meccanismi pratici per il provisioning, in base a questi modelli di distribuzione:

- Distribuzione di massa: il provider di servizi acquisisce i Cisco IP Phone in quantità ed esegue li preprovisioning internamente o acquista unità di personalizzazione remota (RC) da Cisco. I dispositivi vengono quindi rilasciati ai clienti nell'ambito di un contratto di assistenza VoIP.
- Distribuzione al dettaglio: il cliente acquista il Cisco IP Phone da un punto vendita al dettaglio e richiede il servizio VoIP al provider di servizi. Il provider di servizi quindi deve supportare la configurazione remota sicura del dispositivo.

Distribuzione in blocco

In questo modello, il provider di servizi consegna i telefoni ai propri clienti come parte di un contratto di assistenza VoIP. I dispositivi sono unità RC o il preprovisioning viene eseguito internamente.

Cisco esegue il preprovisioning di unità RC per eseguire la risincronizzazione con un server Cisco che scarica gli aggiornamenti del firmware e del profilo del dispositivo.

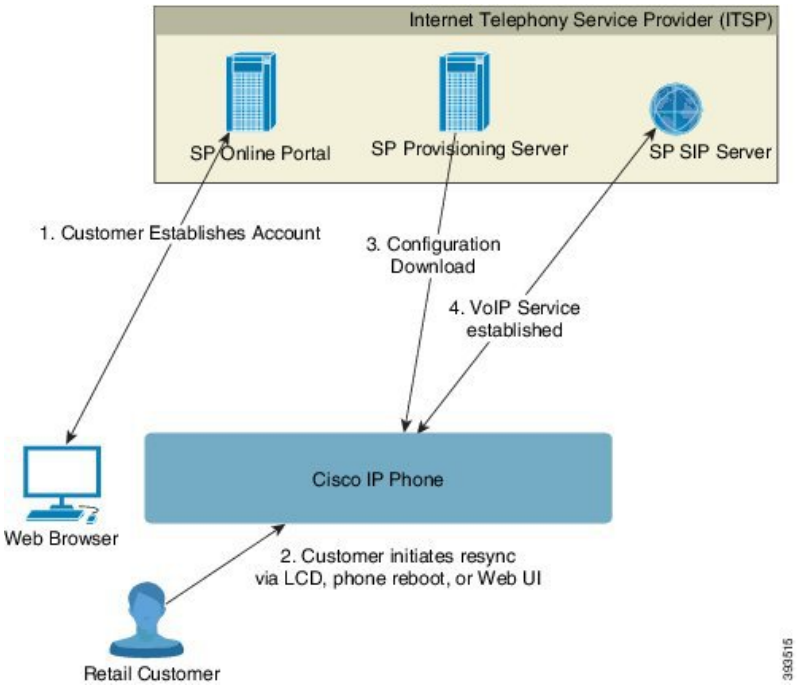
Un provider di servizi può eseguire il preprovisioning dei telefoni con i parametri desiderati, inclusi i parametri che consentono di controllare la risincronizzazione, tramite diversi metodi:

- Internamente tramite DHCP e TFTP
- In remoto tramite TFTP, HTTP o HTTPS
- Una combinazione di provisioning interno e remoto

Distribuzione al dettaglio

In un modello di distribuzione al dettaglio, un cliente acquista un telefono e sottoscrive un particolare servizio. L'Internet Telephony Service Provider (ITSP) consente di impostare e gestire un server di provisioning ed esegue il preprovisioning del telefono per risincronizzarlo con il server del provider di servizi.

Figura 1: Distribuzione al dettaglio



Il telefono include l'utilità di configurazione basata sul Web che visualizza la configurazione interna e accetta nuovi valori dei parametri di configurazione. Il server accetta anche una sintassi di comando URL speciale per l'esecuzione di operazioni di aggiornamento del firmware e di risincronizzazione dei profili remoti.

Il cliente accede al servizio e definisce un account VoIP, eventualmente tramite un portale online e associa il dispositivo all'account del server assegnato. Al telefono del quale non è stato eseguito il provisiong viene richiesto di effettuare la risincronizzazione con un server di provisioning specifico tramite un comando URL di risincronizzazione. In genere, il comando URL include un numero ID del cliente o un codice alfanumerico dell'account per associare il dispositivo al nuovo account.

Nell'esempio seguente, a un dispositivo all'indirizzo IP assegnato tramite DHCP 192.168.1.102 viene richiesto di eseguire l'auto-provisioning al servizio SuperVoIP:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In questo esempio, 1234abcd è il numero ID del cliente del nuovo account. Il server di provisioning remoto associa il telefono che sta eseguendo la richiesta di risincronizzazione al nuovo account, in base all'URL e all'ID cliente fornito. Tramite questa operazione di risincronizzazione iniziale, il telefono è configurato in un'unica fase. Il telefono viene automaticamente indirizzato alla risincronizzazione da quel momento in poi a un URL permanente sul server. Ad esempio:

```
https://prov.supervoip.com/cisco-init
```

Per l'accesso iniziale e permanente, il server di provisioning si basa sul certificato client del telefono per l'autenticazione. Il server di provisioning fornisce i valori dei parametri di configurazione corretti in base all'account del server associato.

Quando si accende il dispositivo o allo scadere di un periodo di tempo specificato, il telefono si risincronizza e scarica i parametri più recenti. Questi parametri possono consentire di conseguire obiettivi quali l'impostazione di un gruppo di ricerca, l'impostazione di numeri di chiamata rapida e la limitazione delle funzioni che un utente può modificare.

Argomenti correlati

Preprovisioning del dispositivo interno, a pagina 43

Processo di risincronizzazione

Il firmware per ciascun telefono include un server Web di amministrazione che accetta i nuovi valori dei parametri di configurazione. Al telefono può essere espressamente chiesto di risincronizzare la configurazione dopo il riavvio, o a intervalli pianificati con un server di provisioning specificato tramite un comando URL di risincronizzazione nel profilo del dispositivo.

Per impostazione predefinita, il server Web è abilitato. Per abilitare o disabilitare il server Web, utilizzare il comando URL di risincronizzazione.

Se necessario, può essere richiesta una risincronizzazione immediata tramite un URL di azione di "risincronizzazione". Il comando URL di risincronizzazione può includere un numero ID del cliente o un codice alfanumerico dell'account per associare in modo univoco il dispositivo all'account dell'utente.

Esempio

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

In questo esempio, a un dispositivo all'indirizzo IP assegnato tramite DHCP 192.168.1.102 viene richiesto di eseguire l'auto-provisioning al servizio SuperVoIP su prov.supervoip.com. Il numero ID del cliente del nuovo account è 1234abcd. Il server di provisioning remoto associa il telefono che sta eseguendo la richiesta di risincronizzazione all'account, in base all'URL e all'ID cliente.

Tramite questa operazione di risincronizzazione iniziale, il telefono è configurato in un'unica fase. Il telefono viene automaticamente indirizzato alla risincronizzazione da quel momento in poi a un URL permanente sul server.

Per l'accesso iniziale e permanente, il server di provisioning si basa sul certificato client per l'autenticazione. Il server fornisce i valori dei parametri di configurazione in base all'account del server associato.

Provisioning

Un telefono può essere configurato per risincronizzare il relativo stato di configurazione interno in modo che corrisponda a un profilo remoto periodicamente e all'accensione. Il telefono contatta un server di provisioning normale (NPS) o un Access Control Server (ACS).

Per impostazione predefinita, una risincronizzazione del profilo viene tentata solo quando il telefono è inattivo. In questo modo si impedisce un aggiornamento che attiverebbe un riavvio del software e interromperebbe una chiamata. Se sono necessari aggiornamenti intermedi per raggiungere uno stato corrente di aggiornamento da una versione precedente, la logica di aggiornamento può automatizzare aggiornamenti multifase.

Normal Provisioning Server

Il Normal Provisioning Server (NPS) può essere un server TFTP, HTTP o HTTPS. Un aggiornamento del firmware remoto si ottiene utilizzando TFTP o HTTP o HTTPS, perché il firmware non contiene informazioni riservate.

Sebbene HTTPS sia raccomandato, la comunicazione con l'NPS non richiede l'uso di un protocollo sicuro perché il profilo aggiornato può essere crittografato utilizzando una chiave segreta condivisa. Per ulteriori informazioni sull'utilizzo di HTTPS, vedere Crittografia delle comunicazioni, a pagina 5. Un provisioning sicuro alla prima connessione che viene fornito tramite un meccanismo che utilizza la funzionalità SSL. Un telefono del quale non è stato eseguito il provisioning può ricevere un profilo crittografato con chiave simmetrica a 256 bit destinata a tale dispositivo.

Controllo dell'accesso di configurazione

Il firmware del telefono fornisce meccanismi per limitare l'accesso degli utenti finali ad alcuni parametri. Il firmware fornisce privilegi specifici per l'accesso a un account **Ammin** o un account **Utente**. Ognuno di essi può essere protetto da password in modo indipendente.

- Account ammin: consente al provider di servizi accesso completo a tutti i parametri del server Web di amministrazione.
- Account utente: consente all'utente di configurare un sottoinsieme di parametri del server Web di amministrazione.

Il fornitore del servizio può limitare l'account utente nel profilo di provisioning nei seguenti modi:

- Indicare quali parametri di configurazione sono disponibili per l'account utente durante la creazione della configurazione.
- Disabilitare l'accesso dell'utente al server Web di amministrazione.
- Disabilitare l'accesso utente per l'interfaccia utente LCD.
- Ignorare la schermata **Imposta password** per l'utente.
- Limitare i domini di Internet accessibili dal dispositivo per risincronizzazione, aggiornamenti o registrazione SIP per la linea 1.

Argomenti correlati

Proprietà di tag elemento, a pagina 16
Controllo degli accessi, a pagina 18

Accesso alla pagina Web del telefono

Se il provider di servizi ha disabilitato l'accesso all'utilità di configurazione, contattarlo prima di continuare.

Procedura

Passaggio 1	Assicurarsi che il computer possa comunicare con il telefono. Nessuna VPN in uso.
Passaggio 2	Avviare un browser Web.
Passaggio 3	Immettere l'indirizzo IP del telefono nella barra degli indirizzi del browser Web.

- Accesso utente: **http://<indirizzo ip>**
- Accesso amministratore: **http://<indirizzo ip>/admin/advanced**
- Accesso amministratore: **http://<indirizzo ip>**, fare clic su **Admin Login**, quindi su **advanced**

Ad esempio, `http://10.64.84.147/admin/`

Passaggio 4 Inserire la password quando richiesto.

Autorizzazione dell'accesso Web a Cisco IP Phone

Per visualizzare i parametri del telefono, abilitare il profilo di configurazione. Per apportare modifiche a qualsiasi parametro, è necessario essere autorizzati a modificare il profilo di configurazione. L'amministratore del sistema potrebbe aver disabilitato l'opzione per rendere l'interfaccia utente Web del telefono visualizzabile o modificabile.

Per ulteriori informazioni, consultare la *Guida per il provisioning dei telefoni multipiattaforma Cisco IP Phone serie 6800*.

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Fare clic su **Voice** > **System**.

Passaggio 2 Nella sezione **System Configuration**, impostare l'opzione **Enable Web Server** su **Yes**.

Passaggio 3 Per aggiornare il profilo di configurazione, fare clic su **Submit All Changes** dopo aver modificato i campi nell'interfaccia utente Web del telefono.

Il telefono viene riavviato e le modifiche vengono applicate.

Passaggio 4 Per annullare tutte le modifiche apportate durante la sessione corrente (o dopo l'ultima volta che è stato fatto clic su **Submit All Changes**), fare clic su **Undo All Changes**. Vengono ripristinati i valori delle impostazioni precedenti.

Procedure di provisioning del telefono

In genere, il Cisco IP Phone è configurato per il provisioning durante la prima connessione alla rete. Il provisioning del telefono viene eseguito anche a intervalli pianificati impostati quando il provider di servizi o il VAR eseguono il preprovisioning (configurano) il telefono. I provider di servizi possono autorizzare i VAR o gli utenti avanzati affinché effettuino il provisioning del telefono manualmente utilizzando la tastiera del telefono. È inoltre possibile configurare il provisioning tramite l'interfaccia utente Web del telefono.

Selezionare **Stato** > **Stato telefono** > **Provisioning** dalla UI LCD del telefono o Stato del provisioning nella scheda **Status** dell'utilità di configurazione basata su Web.

Argomenti correlati

Provisioning manuale di un telefono dalla tastiera, a pagina 11

Onboarding del telefono con il codice di attivazione

Questa funzione è disponibile nella versione del firmware 11-2-3MSR1, BroadWorks Application Server versione 22.0 (patch AP.as.22.0.1123.ap368163 e relative dipendenze). Tuttavia, per utilizzare questa funzione è possibile modificare i telefoni con versioni del firmware meno recenti. Per attivare la schermata del codice di attivazione, è necessario impostare il telefono per l'aggiornamento al nuovo firmware e utilizzare la regola del profilo `gds://`. Per eseguire automaticamente l'onboarding, l'utente immette un codice di 16 cifre nell'apposito campo.

Nota l Telefoni multipiattaforma Cisco IP Phone 6861 non supportano il codice di attivazione per l'onboarding.

Prima di iniziare

Per supportare l'onboarding tramite codice di attivazione, assicurarsi che il servizio activation.webex.com sia consentito dal firewall in uso.

Procedura

Passaggio 1 Modificare il file config.xml in un editor di testo o XML.

Passaggio 2 Per impostare la regola del profilo per l'onboarding tramite codice di attivazione, seguire l'esempio riportato di seguito nel file config.xml.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

Passaggio 3 Salvare le modifiche nel file config.xml.

Provisioning manuale di un telefono dalla tastiera

Procedura

Passaggio 1 Premere **Applicazioni** .

Passaggio 2 Selezionare **Amministrazione dispositivo** > **Regola profilo**.

Passaggio 3 Immettere la regola profilo utilizzando il seguente formato:

```
protocol://server[:port]/profile_pathname
```

Ad esempio:

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

Se non viene specificato alcun protocollo, viene utilizzato il protocollo TFTP. Se non viene specificato alcun nome server, viene utilizzato il nome dell'host che richiede l'URL. Se non viene specificata alcuna porta, viene utilizzata la porta predefinita (69 per TFTP, 80 per HTTP o 443 per HTTPS).

Passaggio 4 Premere **Risincr.**.

Argomenti correlati

Procedure di provisioning del telefono, a pagina 10

Condivisione del firmware

Peer Firmware Sharing (PFS) è un modello di distribuzione del firmware che consente a un Cisco IP Phone di trovare sulla subnet altri telefoni dello stesso modello o della stessa serie e condividere i file del firmware aggiornati quando è necessario eseguire l'aggiornamento di più telefoni contemporaneamente. PFS utilizza Cisco Peer-to-Peer-Distribution Protocol (CPPDP), che è un protocollo proprietario di Cisco. Con il protocollo CPPDP, tutti i dispositivi nella subnet creano una gerarchia peer-to-peer e copiano il firmware o gli altri file dai dispositivi peer ai dispositivi adiacenti. Per ottimizzare gli aggiornamenti del firmware, un telefono principale scarica l'immagine del firmware dal server di caricamento e trasferisce il firmware agli altri telefoni presenti sulla subnet utilizzano le connessioni TCP.

Condivisione del firmware:

- Limita la congestione sui trasferimenti TFTP verso i server di caricamento rimossi a livello centrale.
- Elimina la necessità di controllare manualmente gli aggiornamenti del firmware.
- Riduce le interruzioni dell'operatività del telefono durante gli aggiornamenti mentre è in corso la reimpostazione simultanea di più telefoni

Nota

- La condivisione del firmware funziona soltanto se vengono aggiornati più telefoni contemporaneamente. Quando viene inviato un messaggio NOTIFY con Event:resync, viene avviata una risincronizzazione del telefono. Esempio di un file xml che può contenere le configurazioni per avviare l'aggiornamento:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Quando si imposta il parametro Peer Firmware Sharing Log Server su un indirizzo IP e su una porta, i registri specifici di PFS vengono inviati al server come messaggi UDP. Questa impostazione deve essere eseguita su ogni telefono. È possibile utilizzare i messaggi del registro per la risoluzione dei problemi relativi a PFS.

Peer_Firmware_Sharing_Log_Server consente di specificare il nome host e la porta del server Syslog di UDP Remote. Per impostazione predefinita, la porta è la syslog 514 predefinita.

Ad esempio:

```
<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>
```

Per utilizzare questa funzione, abilitare PFS sui telefoni.

Come ignorare la schermata Imposta password

È possibile ignorare la schermata **Imposta password** del telefono al primo avvio o dopo una ripristino delle impostazioni di fabbrica in base alle seguenti azioni di provisioning:

- Configurazione DHCP
- Configurazione EDOS
- Configurazione della password utente utilizzando il file di configurazione XML del telefono.

Tabella 1: Azioni di provisioning che determinano se viene visualizzata la schermata Imposta password

DHCP configurato	EDOS configurato	Password utente configurata	Ignora schermata Imposta password
Sì	n/d	Sì	Sì
Sì	n/d	No	**No**
No	Sì	Sì	Sì
No	Sì	No	**No**
No	No	n/d	**No**

Procedura

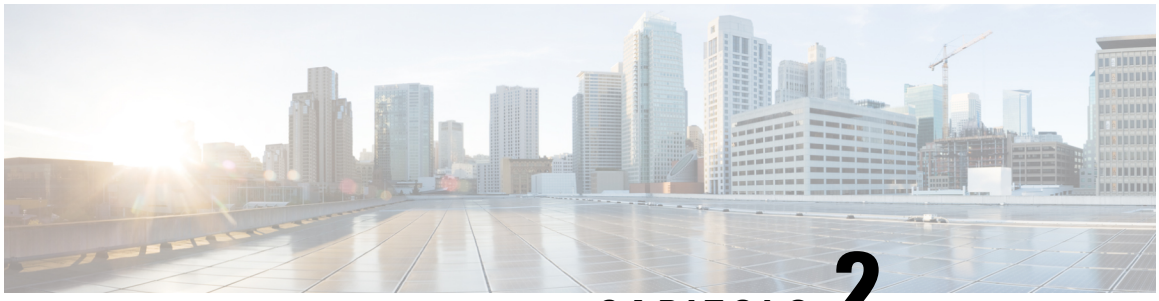
Passaggio 1 Modificare il file `cfg.xml` in un editor di testo o XML.

Passaggio 2 Inserire il tag **<User_Password>** utilizzando una delle seguenti opzioni.

- **Nessuna password (tag di inizio e fine)**–**<User_Password></User_Password>**
- **Valore password (da 4 a 127 caratteri)**–**<User_Password ua="rw">abc123</User_Password>**
- **Nessuna password (solo tag di inizio)**–**<User_Password />**

Passaggio 3 Salvare le modifiche nel file `cfg.xml`.

La schermata **Imposta password** non viene visualizzata al primo avvio o dopo un ripristino delle impostazioni di fabbrica. Se viene specificata una password, all'utente viene chiesto di immettere la password quando accede alla pagina Web del telefono o ai menu dello schermo del telefono.



CAPITOLO 2

Formati di provisioning

Script di provisioning

Il telefono accetta configurazione in formato XML.

Per informazioni dettagliate sul telefono, consultare la Guida all'amministrazione del dispositivo specifico. Ogni guida descrive i parametri che possono essere configurati attraverso il server Web di amministrazione.

Formati dei profili di configurazione

Il profilo di configurazione definisce i valori del parametro per il telefono.

Il formato XM profilo di configurazione utilizza gli strumenti di modifica XML standard per compilare i parametri e i valori.

Nota È supportato solo il set di caratteri UTF-8. Se si modifica il profilo in un editor, non modificare il formato di codifica; in caso contrario, il telefono non sarà in grado di riconoscere il file.

Ogni modello di telefono dispone di un insieme di funzioni diverse e pertanto una serie di parametri diversa.

Profilo (XML) in formato XML

Il profilo in formato Open è un file di testo con sintassi simile a XML che contiene una gerarchia di elementi e i relativi attributi e valori. Questo formato consente di utilizzare gli strumenti standard per creare il file di configurazione. È possibile inviare un file di configurazione in questo formato dal server di provisioning al

telefono durante un'operazione di risincronizzazione. Il file può essere inviato senza compilazione come un oggetto binario.

Il telefono può accettare formati di configurazione che generano gli strumenti standard. Questa funzione facilita lo sviluppo del software del server di provisioning back-end che genera profili di configurazione dai database esistenti.

Per proteggere le informazioni riservate nel profilo di configurazione, il server di provisioning fornisce questo tipo di file al telefono tramite un canale protetto da TLS. Se lo si desidera, il file può essere compresso utilizzando l'algoritmo DEFLATE gzip (RFC1951).

Il file può essere crittografato con uno dei seguenti metodi di crittografia:

- Crittografia AES-256-CBC
- Crittografia dei contenuti HTTP basata su RFC 8188 con codifica AES-128-GCM

Esempio: formato profilo Open

```
<flat-profile>
<Resync_On_Reset> Yes </Resync_On_Reset>
<Resync_Periodic> 7200 </Resync_Periodic>
<Profile_Rule> tftp://prov.telco.com:6900/cisco/config/CP_xxxx_MPP.cfg</Profile_Rule>
</flat-profile>
```

Il tag elemento <flat-profile> racchiude tutti gli elementi di parametro riconosciuti dal telefono.

Argomenti correlati

Compressione e crittografia di un profilo Open (XML), a pagina 20

Componenti dei file di configurazione

Un file di configurazione può includere i seguenti componenti:

- Tag elementi
- Attributi
- Parametri
- Funzioni di formattazione
- Commenti XML

Proprietà di tag elemento

- Il formato di provisioning XML e l'interfaccia utente Web consentono la configurazione delle stesse impostazioni. Il nome del tag XML e i nomi dei campi nell'interfaccia utente Web sono simili ma variano a causa di limitazioni del nome dell'elemento XML. Ad esempio, trattini bassi (_) al posto di " ".
- Il telefono riconosce gli elementi con nomi del parametro corretti incapsulato nell'elemento speciale <flat-profile>.
- I nomi degli elementi sono immessi tra parentesi angolari.

- La maggior parte dei nomi degli elementi sono simili ai nomi dei campi nelle pagine Web di amministrazione per il dispositivo, con le seguenti modifiche:
  - I nomi degli elementi potrebbe non includere spazi o caratteri speciali. Per derivare il nome dell'elemento dal nome del campo amministrazione Web, sostituire un trattino basso per ogni spazio o carattere speciale `[`, `]`, `(`, `)` o `/`.

    Esempio: l'elemento <Resync_On_Reset> rappresenta il campo **Risincronizza dopo reimpostazione** dopo la reimpostazione.
  - Il nome di ogni elemento deve essere univoco. Nelle pagine Web di amministrazione, gli stessi campi possono comparire su più pagine Web, ad esempio le pagine di linea, dell'utente e degli interni. Aggiungere `[n]` al nome dell'elemento per indicare il numero visualizzato nella scheda pagina.

    Esempio: l'elemento <Dial_Plan_1_> rappresenta il **Piano di composizione** per la linea 1.
- Ogni tag elemento di apertura deve avere un corrispondente tag elemento di chiusura. Ad esempio:

```
<flat-profile>
<Resync_On_Reset> Yes
  </Resync_On_Reset>
<Resync_Periodic> 7200
  </Resync_Periodic>
<Profile_Rule>tftp://prov.telco.com: 6900/cisco/config/CP_xxxx_MPP.cfg
  </Profile_Rule>
</flat-profile>
```

- I tag elemento fanno differenza tra maiuscole e minuscole.
- I tag elemento vuoti sono consentiti e vengono interpretati come configurazione del valore vuoto. Immettere il tag dell'elemento di apertura senza un tag di elemento corrispondente e immettere uno spazio e una barra prima della parentesi angolare di chiusura (>). In questo esempio, la regola profilo B è vuota:

```
<Profile_Rule_B />
```

- È possibile utilizzare un tag elemento vuoto per evitare di sovrascrivere i valori forniti dall'utente durante un'operazione di risincronizzazione. Nell'esempio seguente, le impostazioni di chiamata rapida utente restano invariate:

```
<flat-profile>
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
</flat-profile>
```

- Utilizzare un valore vuoto per impostare il parametro corrispondente a una stringa vuota. Immettere un elemento di apertura e chiusura senza alcun valore infrapposto. Nell'esempio seguente, il parametro GPP_A è impostato su una stringa vuota.

```
<flat-profile>
<GPP_A>
  </GPP_A>
</flat-profile>
```

- I nomi di elemento non riconosciuti vengono ignorati.

Argomenti correlati

Controllo dell'accesso di configurazione, a pagina 9

Attributo di accesso utente

I controlli degli attributi (**ua)** dell'accesso utente possono essere utilizzati per modificare l'accesso dall'account utente. Se l'attributo **ua** non è specificato, viene mantenuta l'impostazione di accesso utente esistente. Questo attributo non influisce sull'accesso dell'account ammin.

L'attributo **ua** deve disporre di uno dei seguenti valori:

- na: nessun accesso
- ro: sola lettura
- rw: lettura/scrittura

Nell'esempio seguente viene illustrato l'attributo **ua**:

```
<flat-profile>
   <SIP_TOS_DiffServ_Value_1_ ua=”na”/>
   <Dial_Plan_1_ ua=”ro”/>
   <Dial_Plan_2_ ua=”rw”/>
</flat-profile>
```

Le virgolette doppie devono racchiudere il valore dell'opzione **ua**.

Controllo degli accessi

Se il parametro <Phone-UI-User-Mode> è abilitato, la GUI del telefono garantisce all'attributo di accesso utente i relativi parametri quando l'interfaccia grafica utente visualizza una voce di menu.

Per le voci di menu associate a un parametro di configurazione singolo:

- Fornire il parametro con l'attributo "ua=na" ("ua" significa "accesso utente") rende la voce non più visualizzabile.
- Fornire il parametro con l'attributo "ua=ro" rende la voce di sola lettura e non modificabile.

Per le voci di menu associate a parametri di configurazione multipli:

- Fornire tutti i parametri interessati con l'attributo "ua=na" rende le voci non più visualizzabili.

Argomenti correlati

Controllo dell'accesso di configurazione, a pagina 9

Proprietà parametri

Queste proprietà sono valide per i parametri:

- Tutti i parametri non specificati da un profilo restano invariati nel telefono.
- I parametri non riconosciuti vengono ignorati.
- Se il profilo in formato Open contiene più occorrenze dello stesso tag parametro, l'ultima di tali occorrenze ha la priorità su tutte quelle precedenti. Per evitare la sostituzione accidentale dei valori di configurazione per un parametro, ciascun profilo deve specificare al massimo un'istanza di un parametro.
- L'ultimo profilo elaborato ha la precedenza. Se più profili specificano lo stesso parametro di configurazione, il valore dell'ultimo profilo ha la precedenza.

Formati della stringa

Le seguenti proprietà si applicano alla formattazione delle stringhe:

- Sono consentiti commenti tramite la sintassi XML standard.

  ```
  <!-- My comment is typed here -->
  ```

- Lo spazio vuoto iniziale e finale è consentito per scopi di leggibilità ma viene rimosso dal valore del parametro.
- Le nuove righe all'interno di un valore vengono convertite in spazi.
- Un'intestazione XML del modulo `<? ?>` è consentita, ma il telefono la ignora.
- Per immettere caratteri speciali, utilizzare caratteri di escape XML di base, come illustrato nella tabella riportata di seguito.

Carattere speciale	Sequenza di escape XML
& (e commerciale)	&
< (minore di)	<
> (maggiore di)	>
' (apostrofo)	'
" (virgolette doppie)	"

  Nell'esempio seguente, i caratteri di escape sono immessi per rappresentare i simboli maggiore di e minore di simboli necessari in una regola di piano di numerazione. Questo esempio definisce un piano di numerazione hotline informazioni che consente di impostare il parametro <Dial_Plan_1_ > (**Admin Login** > **advanced** > **Voice** > **Ext (n)**) uguale a (S0 <:18005551212>).

  ```
  <flat-profile>
   <Dial_Plan_1_>
    (S0 <:18005551212>)
   </Dial_Plan_1_>
  </flat-profile>
  ```

- Caratteri numerici di escape, utilizzando i valori decimali ed esadecimali (s.a. `&#40;` e `&#x2e;`), vengono convertiti.

- Il firmware del telefono supporta solo i caratteri ASCII.

Compressione e crittografia di un profilo Open (XML)

Il profilo di configurazione aperto può essere compresso per ridurre il carico di rete sul server di provisioning. Il profilo può, inoltre, essere crittografato per proteggere le informazioni riservate. La compressione non è necessaria, ma deve precedere la crittografia.

Argomenti correlati

Formati dei profili di configurazione, a pagina 15

Compressione di un profilo Open

Il metodo di compressione supportato è l'algoritmo di deflazione gzip (RFC1951). L'utilità gzip e l'archivio di compressione, che implementa lo stesso algoritmo (zlib), sono disponibili da siti Internet.

Per identificare la compressione, il telefono prevede che il file compresso contenga un'intestazione compatibile gzip. La chiamata dell'utilità gzip sul profilo Open originale genera l'intestazione. Il telefono controlla l'intestazione del file scaricato per determinare il formato del file.

Ad esempio, se `profile. XML` è un profilo valido, anche il file `profile.xml.gz` viene accettato. Entrambi i seguenti comandi possono generare questo tipo di profilo:

- `>gzip profile.xml`

  Sostituisce il file originale con il file compresso.

- `>cat profile.xml | gzip > profile.xml.gz`

  Lascia il file originale al suo posto e produce il nuovo file compresso.

Un tutorial sulla compressione è fornito nella sezione Compressione di un profilo Open con Gzip, a pagina 64.

Argomenti correlati

Compressione di un profilo Open con Gzip, a pagina 64

Crittografia di profilo Open

La crittografia a chiave simmetrica può essere utilizzata per crittografare un profilo di configurazione aperto, indipendentemente dalla compressione del file. La compressione, se applicata, deve essere applicata prima della crittografia.

Il server di provisioning utilizza HTTPS per gestire la distribuzione iniziale del telefono dopo la distribuzione. La pre-crittografia dei profili di configurazione non in linea consente l'utilizzo di HTTP per la successiva risincronizzazione dei profili. In questo modo viene ridotto il carico sul server HTTPS nelle distribuzioni su larga scala.

Il telefono supporta due metodi di crittografia per file di configurazione:

- Crittografia AES-256-CBC
- Crittografia dei contenuti HTTP basata su RFC 8188 con codifica AES-128-GCM

Il provisioning nell'unità della chiave o dell'IKM (Input Keying Material) deve essere effettuato in precedenza. Il bootstrap della chiave segreta può essere eseguito in modo protetto tramite HTTPS.

Il nome del file di configurazione non richiede un formato specifico, ma un nome file che termina con l'estensione `.cfg` normalmente indica un profilo di configurazione.

Crittografia AES-256-CBC

Il telefono supporta la crittografia AES-256-CBC per file di configurazione.

Lo strumento di crittografia OpenSSL, disponibile per il download da diversi siti Internet, può eseguire la crittografia. Il supporto per la crittografia AES a 256 bit potrebbe richiedere la ricompilazione dello strumento per abilitare il codice AES. Il firmware è stato testato rispetto alla versione openssl-0.9.7c.

Crittografia di un profilo con OpenSSL, a pagina 65 fornisce un tutorial sulla crittografia.

Per un file crittografato, il profilo prevede il file abbia lo stesso formato in maniera analoga a quello generato dal seguente comando:

```
# example encryption key = SecretPhrase1234

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml -out profile.cfg

# analogous invocation for a compressed xml file

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml.gz -out profile.cfg
```

Una -k minuscola precede la chiave segreta, la quale può essere una frase di testo vuota utilizzata per generare un salt a 64 bit casuale. Con la chiave segreta specificata dall'argomento -k, lo strumento di crittografia richiama un vettore casuale a 128 bit iniziale e la corrente chiave di crittografia a 256 bit.

Quando la suddetta forma di crittografia è impiegata in un profilo di configurazione, è necessario che il telefono riceva un valore chiave per decriptare il file. Questo valore è specificato come qualificatore nel profilo URL. La sintassi è la seguente, utilizzando un URL esplicito:

```
[--key "SecretPhrase1234"] http://prov.telco.com/path/profile.cfg
```

Questo valore è programmato utilizzando uno dei parametri Profile_Rule.

Argomenti correlati

Crittografia di un profilo con OpenSSL, a pagina 65

Espansione macro

Prima di essere valutati, i diversi parametri di provisioning sono sottoposti a espansione macro interna. Questo passaggio di pre-valutazione fornisce maggiore flessibilità nel controllo delle attività di risincronizzazione e aggiornamento del telefono.

Questi gruppi di parametri sono sottoposti a espansione macro prima della valutazione:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

In determinate condizioni, anche alcuni parametri generici (GPP_*) sono sottoposti a espansione macro, come indicato in modo esplicito in Argomenti di risincronizzazione opzionali, a pagina 25.

Durante l'espansione macro, il contenuto di variabili denominate sostituisce espressioni della forma $NAME e $(NAME). Queste variabili includono parametri generici, diversi identificatori di prodotto, alcuni timer di evento e valori dello stato di provisioning. Per un elenco completo, vedere Variabili espansione macro, a pagina 77.

Nell'esempio seguente, l'espressione $(MAU) viene utilizzata per immettere l'indirizzo MAC 000E08012345.

L'amministratore immette: **`$(MAU)config.cfg`**

L'espansione macro risultante per un dispositivo con indirizzo MAC MAC000E08012345 è:
`000E08012345config.cfg`

Se un nome macro non viene riconosciuto, rimane compresso senza essere esteso. Ad esempio, il nome STRANGE non è riconosciuto come nome macro valido, mentre MAU è riconosciuto come nome macro valido.

L'amministratore immette: **`$STRANGE$MAU.cfg`**

L'espansione macro risultante per un dispositivo con indirizzo MAC MAC000E08012345 è:
`$STRANGE000E08012345.cfg`

L'espansione macro non viene applicata in modo ricorsivo. Ad esempio, $$MAU" si estende in $MAU" ($$ viene espanso) e non si ottiene l'indirizzo MAC.

Il contenuto dei parametri per scopi speciali, GPP_SA tramite GPP_SD, è associato alle espressioni di macro $SA tramite $SD. I parametri riportati di seguito sono solo con macro estesa come argomento **--key**, le opzioni **--uid** e **--pwd** in un URL risincronizzato.

Espressioni condizionali

Le espressioni condizionali possono generare eventi di risincronizzazione e selezionare da URL alternativi per le operazioni di sincronizzazione e aggiornamento.

Le espressioni condizionali sono composte da un elenco di confronti, separati da **e** operatore. Tutti i confronti devono essere soddisfatti affinché la condizione sia true.

Ogni confronto può essere correlato a uno dei seguenti tre tipi di letterali:

- Valori interi
- Numeri di versione hardware o software
- Stringhe con virgolette doppie

Numeri di versione

La versione del software formale dei telefoni multipiattaforma (MPP) utilizza questo formato, dove BN = numero di build:

- Cisco IP Phone serie 6800:`sip68xx.v1-v2-v3MPP-BN`

La stringa di confronto deve utilizzare lo stesso formato. In caso contrario, si verificherà un errore di analisi formato.

Nella versione del software, v1-v2-v3-v4 può specificare diversi cifre e caratteri, ma deve iniziare con una cifra numerica. Durante il confronto della versione del software, v1-v2-v3-v4 viene confrontato in sequenza e le cifre più a sinistra hanno la precedenza sulle ultime.

Se v[x] include solo valori numerici, le cifre vengono confrontate; se v[x] include cifre numeriche + caratteri alfabetici, vengono confrontate prima le cifre, quindi vengono confrontati i caratteri in ordine alfabetico.

Esempio di numero di versione valido

sipyyyy.11-0-0MPP-BN

Al contrario: 11.0.0 è un formato non valido.

Confronto

sip68xx.11-0-0MPP-BN < sip68xx.11-0-1MPP-BN

Le stringhe tra virgolette possono essere confrontate per uguaglianza o disuguaglianza. Numeri di versione e numeri interi possono inoltre essere confrontati in maniera aritmetica. Gli operatori di confronto possono essere espressi come simboli o come acronimi. Gli acronimi sono pratici per esprimere la condizione in un profilo in formato Open.

Operatore	Sintassi alternativa	Descrizione	Applicabile a numeri interi e operandi della versione	Applicabile a operandi in stringhe tra virgolette
=	eq	uguale a	Sì	Sì
!=	ne	non uguale a	Sì	Sì
<	lt	è minore di	Sì	No
<=	le	è minore o uguale a	Sì	No
>	gt	è maggiore di	Sì	No
>=	ge	è maggiore o uguale a	Sì	No
E		e	Sì	Sì

È importante racchiudere variabili macro tra virgolette doppie ove si attende una stringa letterale. Non eseguire tale azione quando si attende un numero o un numero di versione.

Quando utilizzate nel contesto di parametri Profile_Rule* e Upgrade_Rule, le espressioni condizionali devono essere racchiuse tra la sintassi "(espress)?" come in questo esempio di regola di aggiornamento. Tenere presente che BN significa "numero di build".

```
($SWVER ne sip68xx.11-0-0MPP)? http://ps.tell.com/sw/sip68xx.11-0-0MPP-BN.loads
```

Non utilizzare la sintassi precedente tra parentesi per configurare i parametri Resync_Trigger_*.

Sintassi dell'URL

Utilizzare la sintassi dell'URL standard per specificare la modalità di ripristino dei file di configurazione e dei carichi del firmware rispettivamente nei parametri Profile_Rule * e Upgrade_Rule. La sintassi è determinata nel seguente modo:

[scheme://] [server [:port]] filepath

Dove **scheme** è uno dei seguenti valori:

- tftp
- http
- https

Se **scheme** è omesso, viene utilizzato il protocollo tftp. Il server può essere un nome host riconosciuto da DNS o un indirizzo IP numerico. La porta è il numero di porta di destinazione UDP o TCP. Il percorso file deve iniziare con una directory principale (/); deve essere un percorso assoluto.

Se **server** è assente, viene usato il sever tftp specificato tramite DHCP (opzione 66).

Nota Per le regole di aggiornamento, è necessario specificare il server.

Se **port** è assente, viene usata la porta standard per lo schema specificato. Tftp utilizza la porta UDP 69, http utilizza la porta TCP 80, https utilizza la porta TCP 443.

Deve essere presente un percorso file. Non deve fare riferimento necessariamente a un file statico ma può indicare contenuto dinamico ottenuto tramite CGI.

L'espansione macro si applica all'interno degli URL. I seguenti sono esempi di URL validi:

```
/$MA.cfg
/cisco/cfg.xml
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

Se si utilizza l'opzione DHCP 66, le regole di aggiornamento non supportano la sintassi vuota. È applicabile solo per Regola profilo.*

Crittografia dei contenuti HTTP basata su RFC 8188

Il telefono supporta la crittografia dei contenuti HTTP basata su RFC 8188 con cifratura AES-128-GCM per i file di configurazione. Con questo metodo di crittografia, qualsiasi entità può leggere le intestazioni dei messaggi HTTP. Tuttavia, solo le entità che conoscono l'IKM (Input Keying Material) possono leggere il payload. Se il telefono è configurato con l'IKM, il telefono e il server di provisioning possono scambiare file di configurazione in modo sicuro e consentire agli elementi di rete di terze parti di utilizzare le intestazioni dei messaggi per scopi di analisi e monitoraggio.

Il parametro di configurazione XML **IKM_HTTP_Encrypt_Content** conserva l'IKM sul telefono. Per motivi di sicurezza, questo parametro non è accessibile dalla pagina Web di amministrazione del telefono. Inoltre non è visibile nel file di configurazione del telefono, accessibile dall'indirizzo IP del telefono o dai report di configurazione del telefono inviati al server di provisioning.

Se si desidera utilizzare la crittografia basata su RFC 8188, verificare quanto segue:

- Effettuare il provisioning del telefono con l'IKM specificando l'IKM con il parametro XML **IKM_HTTP_Encrypt_Content** nel file di configurazione inviato dal server di provisioning al telefono.
- Se la crittografia viene applicata ai file di configurazione inviati dal server di provisioning al telefono, assicurarsi che l'intestazione HTTP *Content-Encoding* presente nel file di configurazione sia «aes128gcm».

  In assenza di questa intestazione, il metodo AES-256-CBC ha la precedenza. Il telefono si applica la decrittografia se è presente una chianve AES-256-CBC in una regola profilo, indipendentemente dall'IKM.
- Se si desidera che il telefono applichi la crittografia ai report di configurazione che invia al server di provisioning, assicurarsi che nella regola di report non sia stata specificata la chiave AES-256-CBC.

Argomenti di risincronizzazione opzionali

Gli argomenti opzionali, **key**, **uid** e **pwd**, possono precedere gli URL immessi nei parametri in Profile_Rule*, collettivamente racchiusi da parentesi quadre.

key

L'opzione **--key** indica al telefono che il file di configurazione ricevuto dal server di provisioning è crittografato con crittografia AES-256-CBC, a meno che nell'intestazione *Content-Encoding* del file sia indicata la crittografia «aes128gcm». La chiave stessa è specificata come una stringa che segue il termine **--key**. Se lo si desidera, è possibile racchiudere la chiave di crittografia tra virgolette ("). Il telefono utilizza il tasto per la decrittografia del file di configurazione.

Esempi d'uso

```
[--key VerySecretValue]
[--key "my secret phrase"]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

Gli argomenti tra parentesi presentano macro estese. I parametri con scopo speciale, da GPP_SA a GPP_SD, sono macro espandibili in variabili macro, da $SA a $SD, solo quando vengono utilizzati come argomenti dell'opzione chiave. Vedere i seguenti esempi:

```
[--key $SC]
[--key "$SD"]
```

Nei profili di formato Open, l'argomento per **--key** deve essere uguale a quello per l'opzione **-k** assegnata a **openssl**.

uid e pwd

Le opzioni **uid** e **pwd** possono essere utilizzate per specificare l'autenticazione dell'ID utente e della password per l'URL specificato. Gli argomenti tra parentesi presentano macro estese. I parametri con scopo speciale, da GPP_SA a GPP_SD, sono macro espandibili in variabili macro, da $SA a $SD, solo quando vengono utilizzati come argomenti dell'opzione chiave. Vedere i seguenti esempi:

```
GPP_SA = MyUserID
GPP_SB = MySecretPassword
```

[--uid $SA -pwd $SB] https://provisioning_server_url/path_to_your_config/your_config.xml

si estende quindi in:

[--uid MyUserID -pwdMySecretPassword]
https://provisioning_server_url/path_to_your_config/your_config.xml

Applicazione di un profilo per il dispositivo di telefonia IP

Dopo aver creato uno script di configurazione XML, è necessario passarlo al telefono per l'applicazione. Per applicare la configurazione, è possibile scaricare sia il file di configurazione per il telefono da un server TFTP, HTTP o HTTPS utilizzando un browser Web o utilizzando l'utilità a riga di comando cURL.

Download del file di configurazione per il telefono da un server TFTP

Seguire queste fasi per scaricare il file di configurazione di un'applicazione su un server TFTP sul proprio PC.

Procedura

Passaggio 1 Connettere il PC alla LAN del telefono.

Passaggio 2 Eseguire un'applicazione server TFTP sul PC e assicurarsi che il file di configurazione sia disponibile nella directory principale TFTP.

Passaggio 3 In un browser Web, immettere l'indirizzo IP della LAN del telefono, l'indirizzo IP del computer, il nome del file e le credenziali di accesso. Utilizzare il seguente formato:

http://<WAN_IP_Address>/admin/resync?tftp://<PC_IP_Address>/<file_name>&xuser=admin&xpassword=<password>

Esempio:

```
http://192.168.15.1/admin/resync?tftp://192.168.15.100/my_config.xml&xuser=admin&xpassword=admin
```

Download del file di configurazione per il telefono utilizzando cURL

Per scaricare la configurazione del telefono utilizzando cURL, procedere nel seguente modo. Questo strumento a riga di comando è utilizzato per il trasferimento dei dati con una sintassi URL. Per scaricare cURL, visitare:

https://curl.haxx.se/download.html

Nota Si consiglia di non utilizzare cURL per registrare la configurazione sul telefono, poiché il nome utente e la password potrebbero essere acquisiti durante l'operazione.

Procedura

Passaggio 1 Collegare il PC alla porta LAN del telefono.

Passaggio 2 Per scaricare il file di configurazione sul telefono, immettere il seguente comando cURL:

```
curl –d @my_config.xml
“http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin”
```

Parametri di provisioning

In questa sezione vengono descritti i parametri di provisioning ampiamente organizzati in base alle funzione:

Esistono questi tipi di parametri di provisioning:

- Per scopi generici
- Caratteristica
- Fattori determinanti
- Pianificazioni configurabili
- Regole di profilo
- Regola di aggiornamento

Parametri per scopi generici

I parametri per scopi generici GPP_* (**Admin Login** > **advanced** > **Voice** > **Provisioning**) vengono utilizzati come stringhe libere e registrati durante la configurazione del telefono per interagire con una specifica soluzione server di provisioning. I parametri GPP_* sono vuoti per impostazione predefinita. Possono essere configurati per contenere diversi valori, inclusi i seguenti:

- Chiavi di crittografia
- URL
- Informazioni sullo stato del provisioning multifase
- Modelli di richiesta POST
- Mappe alias dei nomi dei parametri
- Valori stringa parziali, eventualmente combinati in valori parametro completi.

I parametri GPP_* sono disponibili per l'espansione macro all'interno di altri parametri di provisioning. A tale scopo, i nomi delle macro a singola lettera in maiuscolo (da A a P) sono sufficienti per identificare il contenuto da GPP_A a GPP_P. Inoltre, i nomi delle macro a due lettere maiuscole da SA a SD identificano da GPP_SA a GPP_SD come un caso speciale quando viene utilizzato come argomenti delle opzioni URL seguenti:

key, **uid** e **pwd**

Questi parametri possono essere utilizzati come variabili nelle regole di aggiornamento e provisioning. Essi sono identificati applicando un prefisso al nome della variabile con un carattere "$", ad esempio $GPP_A.

Utilizzo di parametri per scopi generici

Ad esempio, se GPP_A contiene la stringa ABC e GPP_B contiene 123, l'espressione macro AB si estende in ABC123.

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Selezionare **Voice** > **Provisioning**.

Passaggio 2 Scorrere fino alla sezione **General Purpose Parameters**.

Passaggio 3 Immettere i valori validi nei campi, da GPP A a GPP P.

Passaggio 4 Fare clic su **Submit All Changes**.

Caratteristica

I parametri Provision_Enable e Upgrade_Enable controllano tutte le operazioni di risincronizzazione profilo e di aggiornamento del firmware. Tali parametri controllano le risincronizzazioni e gli aggiornamenti indipendentemente le une dagli altri. Questi parametri controllano anche i comandi di risincronizzazione e aggiornamento degli URL che vengono inviati tramite il server Web di amministrazione. Entrambi i parametri riportati di seguito sono impostati su **Sì** per impostazione predefinita.

Il parametro Resync_From_SIP controlla le richieste di operazioni di risincronizzazione. Un evento notifica SIP viene inviato dal server proxy del provider di servizi al telefono. Se abilitato, il proxy può richiedere una risincronizzazione. A tal fine, il proxy invia un messaggio di notifica SIP contenente l'evento: risincronizzazione dell'intestazione al dispositivo.

Il dispositivo risponde alla richiesta con un messaggio 401 (autorizzazione rifiutata per le credenziali utilizzate). Il dispositivo si aspetta una richiesta successiva autenticata prima di rispettare la richiesta di risincronizzazione dal proxy. Gli eventi: reboot_now e Event: restart_now headers eseguono riavvi a freddo e a caldo, rispettivamente, i quali sono altrettanto contestati.

I due restanti abilitati sono Resync_On_Reset e Resync_After_Upgrade_Attempt. Questi parametri determinano se il dispositivo esegue un'operazione di risincronizzazione dopo l'avvio del software in uso e dopo l'aggiornamento di ogni tentativo.

Quando l'opzione Resync_On_Reset è abilitata, il dispositivo fornisce un ritardo casuale che segue la sequenza di avvio prima di eseguire il ripristino. Il ritardo è un'ora casuale fino al valore specificato da Resync_Random_Delay (in secondi). In un gruppo di telefoni che si accendono contemporaneamente, tale ritardo si estende alle ore di inizio delle richieste di risincronizzazione da ciascuna unità. Questa funzione può essere utile in un'ampia distribuzione residenziale, in caso di guasto all'alimentazione regionale.

Fattori determinanti

Il telefono consente di risincronizzazione a intervalli specifici o a un orario specifico.

Risincronizzazione a intervalli specifici

Il telefono è progettato per eseguire la risincronizzazione periodica con il server di provisioning. L'intervallo di risincronizzazione è configurato in Resync_Periodic (secondi). Se questo valore è vuoto, il dispositivo non esegue la risincronizzazione periodica.

La risincronizzazione in genere viene eseguita quando le linee vocali sono inattive. Quando una linea voce è attiva e deve essere eseguita una risincronizzazione, il telefono ritarda la procedura di risincronizzazione finché la linea non diventa inattiva. Una risincronizzazione può causare la modifica dei valori dei parametri di configurazione.

Un'operazione di risincronizzazione non riesce in quanto il telefono non riesce a ripristinare un profilo dal server, il file scaricato è danneggiato o si è verificato un errore interno. Il dispositivo tenta nuovamente la risincronizzazione dopo un tempo specificato in Resync_Error_Retry_Delay (secondi). Se Resync_Error_Retry_Delay è impostato su 0, il dispositivo non tenta di risincronizzarsi dopo un tentativo di risincronizzazione non riuscito.

Se un aggiornamento non riesce, un nuovo tentativo viene eseguito dopo Upgrade_Error_Retry_Delay secondi.

Due parametri configurabili sono disponibili per attivare in modo condizionale una risincronizzazione: Resync_Trigger_1 e Resync_Trigger_2. Ogni parametro può essere programmato con un'espressione condizionale che viene sottoposta a espansione macro. Quando l'intervallo di risincronizzazione scade (tempo per la risincronizzazione successiva), gli elementi attivatori, se impostati, impediranno la risincronizzazione a meno che uno di questi elementi sia stimato true.

La condizione di esempio seguente attiva una risincronizzazione. Nell'esempio, sono già trascorsi più di 5 minuti dall'ultimo tentativo di aggiornamento del telefono (300 secondi) e almeno 10 minuti (600 secondi) dall'ultimo tentativo di risincronizzazione.

```
$UPGTMR gt 300 and $PRVTMR ge 600
```

Risincronizzazione a un orario specifico

Il parametro Resync_At consente al telefono di risincronizzarsi a un orario specifico. Questo parametro utilizza il formato di 24 ore (hhmm) per specificare l'ora.

Il parametro Resync_At_Random_Delay consente al telefono di risincronizzarsi con un ritardo non specificato nel tempo. Questo parametro utilizza un formato di numeri interi positivi per specificare l'ora.

È necessario evitare di sovraccaricare il server con richieste di risincronizzazione di più telefoni impostati per la risincronizzazione alla stessa ora. A tal fine, il telefono attiva la risincronizzazione fino a 10 minuti dopo il tempo specificato.

Ad esempio, se si imposta il tempo di risincronizzazione a 1000 (10:00), il telefono attiva la risincronizzazione in qualsiasi momento tra 10:00 e le ore 10:10.

Per impostazione predefinita, questa funzione è disabilitata. Quando viene predisposta questa funzione, il parametro Resync_At viene ignorato.

Pianificazioni configurabili

È possibile configurare le pianificazioni per risincronizzazioni periodiche ed è possibile specificare gli intervalli di nuovi tentativi per errori di risincronizzazione e di aggiornamento utilizzando i parametri di provisioning riportati di seguito:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Ogni parametro accetta un singolo valore di ritardo (secondi). La nuova sintassi estesa consente un elenco separato da virgole di elementi di ritardi consecutivi. L'ultimo elemento nella sequenza in modo implicito viene ripetuto per sempre.

Se lo si desidera, è possibile utilizzare un segno più per specificare un altro valore numerico che aggiunge un ritardo casuale aggiuntivo.

Esempio 1

In questo esempio, il telefono si risincronizza periodicamente ogni 2 ore. Se si verifica un errore di risincronizzazione, il dispositivo tenta con i seguenti intervalli: 30 minuti, 1 ora, 2 ore e 4 ore. Il dispositivo continua a provare a intervalli di 4 ore fino a quando non riesce a eseguire la risincronizzazione.

```
Resync_Periodic=7200
Resync_Error_Retry_Delay=1800,3600,7200,14400
```

Esempio 2

In questo esempio, il dispositivo periodicamente si risincronizza ogni ora (più un ritardo casuale aggiuntivo fino a 10 minuti). Nel caso di un errore di risincronizzazione, il dispositivo esegue tentativi con i seguenti intervalli: 30 minuti (più fino a 5 minuti). 1 ora (più un massimo di 10 minuti), 2 ore (più un massimo di 15 minuti). Il dispositivo continua a provare a intervalli di 2 (più un massimo di 15 minuti) fino a quando non riesce a risincronizzarsi.

```
Resync_Periodic=3600+600
Resync_Error_Retry_Delay=1800+300,3600+600,7200+900
```

Esempio 3

In questo esempio, se un tentativo di aggiornamento remoto non riesce, il dispositivo tenta l'aggiornamento entro 30 minuti, quindi nuovamente dopo un'ora più, quindi due ore. Se il problema persiste, il dispositivo tenta ogni quattro-cinque ore fino a quando non viene eseguito correttamente l'aggiornamento.

```
Upgrade_Error_Retry_Delay  =  1800,3600,7200,14400+3600
```

Regole di profilo

Il telefono fornisce più parametri per i profili di configurazione remota (Profile_Rule *). Ciascuna operazione di risincronizzazione può ripristinare più file, potenzialmente gestiti da diversi server.

Nello scenario più semplice, il dispositivo si risincronizza periodicamente con un singolo profilo su un server centrale che aggiorna tutti i parametri interni pertinenti. In alternativa, è possibile suddividere il profilo tra i diversi file. Un file è comune per tutti i telefoni in una distribuzione. Viene fornito un file univoco e separato per ogni account. Le chiavi di crittografia e le informazioni possono essere fornite da un ulteriore profilo archiviato su un server separato.

Ogni volta che un'operazione di risincronizzazione è prevista, il telefono valuta i quattro parametri Profile_Rule * in sequenza:

1. Profile_Rule
2. Profile_Rule_B
3. Profile_Rule_C
4. Profile_Rule_D

Ogni valutazione può causare un ripristino profilo da un server di provisioning remoto, con un aggiornamento possibile di un certo numero di interni parametri. Se una valutazione non viene eseguita correttamente, la sequenza di risincronizzazione viene interrotta e viene ritentata nuovamente dall'inizio specificato dal parametro Resync_Error_Retry_Delay (secondi). Se tutte le valutazioni vengono eseguite correttamente, il dispositivo attende il secondo specificato dal parametro Resync_Periodic e quindi esegue un'altra risincronizzazione.

I contenuti di ciascun parametro Profile_Rule* sono costituiti da una serie di alternative. Le alternative sono separate dal carattere | (pipe). Ogni alternativa è costituita da un'espressione condizionale, un'espressione di assegnazione, un URL di profilo e le opzioni URL associate. Tutti questi componenti sono opzionali all'interno di ogni alternativa. Di seguito vi sono le combinazioni valide e l'ordine in cui devono essere visualizzati, se presente:

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

All'interno di ogni parametro Profile_Rule*, tutte le alternative eccetto l'ultima devono fornire un'espressione condizionale. Questa espressione viene valutata ed elaborata nel modo seguente:

1. Le condizioni vengono valutate da sinistra a destra, fino a quando ne viene trovata una ritenuta true (o fino a quando non viene trovata un'alternativa senza alcuna espressione condizionale).
2. Qualsiasi espressione di assegnazione allegata viene valutata, se presente.
3. Se viene specificato un URL come parte di tale alternativa, si tenta di scaricare il profilo che si trova all'URL specificato. Il sistema tenta di conseguenza di aggiornare i parametri interni.

Se tutte le alternative sono espressioni condizionali e nessuna viene valutata come true (o se l'intera regola profilo è vuota), l'intero parametro Profile_Rule* viene ignorato. Il parametro regola profilo successivo nella sequenza viene valutato.

Esempio 1

In questo esempio si risincronizza in modo incondizionato con il profilo all'URL specificato ed esegue una richiesta HTTP GET al server di provisioning remoto:

```
http://remote.server.com/cisco/$MA.cfg
```

Esempio 2

In questo esempio, il dispositivo si risincronizza con due URL diversi, in base allo stato di registrazione della linea 1. In caso di interruzione registrazione, il dispositivo esegue un POST HTTP su uno script CGI. Il dispositivo invia il contenuto della macro estesa GPP_A, che può fornire ulteriori informazioni sullo stato dispositivo:

```
($PRVTMR ge 600)? http://p.tel.com/has-reg.cfg
| [--post a] http://p.tel.com/lost-reg?
```

Esempio 3

In questo esempio, il dispositivo si risincronizza con lo stesso server. Se nell'unità (per unità pre-2.0 legacy) non è installato un certificato, il dispositivo fornisce informazioni aggiuntive:

```
("$CCERT" eq "Installed")? https://p.tel.com/config?
| https://p.tel.com/config?cisco$MAU
```

Esempio 4

In questo esempio, la linea 1 è disabilitata fino a quando GPP_A è uguale a Provisioned (fornito) tramite il primo URL. Successivamente, si risincronizza con il secondo URL:

```
("$A" ne "Provisioned")? (Line_Enable_1_ = "No";)! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

Esempio 5

In questo esempio, il profilo che restituisce il server si presume contenga tag di elementi XML. È necessario eseguire nuovamente il mapping questi tag per i nomi dei parametri corretti dalla mappa degli alias archiviata in GPP_B:

```
[--alias b] https://p.tel.com/account/$PN$MA.xml
```

Una risincronizzazione viene tipicamente considerata come non riuscita se il server non riceve un profilo richiesto. Il parametro Resync_Fails_On_FNF può ignorare questo comportamento predefinito. Quando Resync_Fails_On_FNF è impostato su No, il dispositivo accetta una risposta file-not-found (file non trovato) dal server come risincronizzazione riuscita. Il valore predefinito per Resync_Fails_On_FNF è Sì.

Regola di aggiornamento

La regola di aggiornamento indica il dispositivo da attivare su un nuovo carico e da dove ripristinare il carico, se necessario. Se il carico si trova già sul dispositivo, non tenterà di ottenere il carico. Pertanto, la validità della posizione carico non importa quando il carico desiderato è nella partizione inattiva.

Il parametro Upgrade_Rule specifica un carico del firmware che, se diverso dal carico corrente, verrà scaricato e applicato a meno che non limitato da un'espressione condizionale o Upgrade_Enable è impostato su **No**.

Il telefono fornisce un parametro di aggiornamento configurabile remoto, Upgrade_Rule. Questo parametro accetta la sintassi simile ai parametri della regola del profilo. Le opzioni URL non sono supportate per gli

aggiornamenti, ma è possibile utilizzare espressioni condizionali ed espressioni di assegnazione. Se le espressioni condizionali vengono utilizzate, il parametro può essere popolato con più alternative, separate dal carattere | . La sintassi di ogni alternativa è la seguente:

```
[ conditional-expr ] [ assignment-expr ] URL
```

Come nel caso dei parametri Profile_Rule*, il parametro Upgrade_Rule valuta ogni alternativa fino a quando non è soddisfatta un'espressione condizionale o un'alternativa non ha espressioni condizionali. Qualsiasi espressione di assegnazione allegata viene valutata, se specificata. Quindi, viene tentato un aggiornamento all'URL specificato.

Se Upgrade_Rule contiene un URL senza un'espressione condizionale, il dispositivo verrà aggiornato all'immagine del firmware che specifica l'URL. Dopo l'espansione della macro e la valutazione della regola, il dispositivo non tenta di nuovo di eseguire l'aggiornamento fino a quando non viene modificata la regola o la combinazione reale di schema + server + porta + percorso file.

Per tentare un aggiornamento del firmware, il dispositivo disattiva l'audio all'inizio della procedura e lo riavvia al termine della procedura. Il dispositivo inizia automaticamente un aggiornamento guidato dal contenuto di Upgrade_Rule solo se tutte le linee vocali sono attualmente inattive.

Ad esempio:

- Per Cisco IP Phone serie 6800:

  ```
  http://p.tel.com/firmware/sip68xx.11-1-0MPP-BN.loads

  where BN==Build Number
  ```

In questo esempio, il parametro Upgrade_Rule aggiorna il firmware all'immagine che archiviata all'URL indicato.

Questo è un altro esempio per Cisco IP Phone serie 6800:

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads
| http://p.tel.com/firmware/sip68xx.11-0-1MPP-BN.loads

where BN==Build Number
```

In questo esempio si indirizza l'unità a caricare una delle due immagini, in base al contenuto di un parametro con scopo generico, GPP_F.

Il dispositivo può applicare un limite di downgrade relativo al numero di revisione del firmware, che può essere un'opzione di personalizzazione utile. Se è configurato un numero di revisione del firmware valido nel parametro Downgrade_Rev_Limit, il dispositivo rifiuta i tentativi di aggiornamento per le versioni del firmware precedenti rispetto al limite specificato.

Tipi di dati

Questi tipi di dati vengono utilizzati con parametri di configurazione profilo:

- {a,b,c,…}: a scelta tra a, b, c, …
- Bool: valore booleano "sì" o "no".

- CadScript: un miniscript che consente di specificare i parametri di cadenza di un segnale. Fino a 127 caratteri.

  Sintassi: S_1[; S_2], dove:

  - S_i=D_i($on_{i,1}$/$off_{i,1}$[,$on_{i,2}$/$off_{i,2}$[,$on_{i,3}$/$off_{i,3}$[,$on_{i,4}$/$off_{i,4}$[,$on_{i,5}$/$off_{i,5}$[,$on_{i,6}$/$off_{i,6}$]]]]]) noto come sezione.
  - $on_{i,j}$ e $off_{i,j}$ sono durata attivato/disattivato in secondi di un *segmento*. i = 1 o 2 e j = da 1 a 6.
  - D_i è la durata totale della sezione in secondi.

  Tutte le durate possono avere fino a tre posizioni decimali per fornire una risoluzione di 1 ms. Il carattere jolly "*" indica una durata infinita. I segmenti all'interno di una sezione vengono riprodotti in ordine e ripetuti fino a quando non viene riprodotta la durata totale.

  Esempio 1:

  ```
  60(2/4)

  Number of Cadence Sections = 1
  Cadence Section 1: Section Length = 60 s
  Number of Segments = 1
  Segment 1: On=2s, Off=4s

  Total Ring Length = 60s
  ```

  Example 2—Distinctive ring (short,short,short,long):

  ```
  60(.2/.2,.2/.2,.2/.2,1/4)

  Number of Cadence Sections = 1
  Cadence Section 1: Section Length = 60s
  Number of Segments = 4
  Segment 1: On=0.2s, Off=0.2s
  Segment 2: On=0.2s, Off=0.2s
  Segment 3: On=0.2s, Off=0.2s
  Segment 4: On=1.0s, Off=4.0s

  Total Ring Length = 60s
  ```

- DialPlanScript: sintassi dello script che consente di specificare i piani di numerazione della linea 1 e della linea 2.
- Float<n>: un valore con massimo n decimali in virgola mobile.
- FQDN: nome di dominio completo. Può contenere un massimo di 63 caratteri. Di seguito sono riportati alcuni esempi:
  - sip.Cisco.com:5060 o 109.12.14.12:12345
  - sip.Cisco.com o 109.12.14.12
- FreqScript: un miniscript che specifica i parametri di frequenza e di livello di un segnale. Contiene un massimo di 127 caratteri al massimo.

  Sintassi: F_1@L_1[, F_2@L_2[, F_3@L_3[, F_4@L_4[, F_5@L_5[, F_6@L_6]]]], dove:

  - F_1-F_6 sono frequenze in Hz (solo numeri interi senza segni).

- L_1– L_6 sono i corrispondenti livelli in dBm (con un massimo di una posizione decimale).

Gli spazi vuoti prima e dopo la virgola sono consentiti ma non consigliati.

Esempio 1: segnale di chiamata in attesa:

```
440@-10

Number of Frequencies = 1
Frequency 1 = 440 Hz at –10 dBm
```

Esempio 1: segnale di linea:

```
350@-19,440@-19

Number of Frequencies = 2
Frequency 1 = 350 Hz at –19 dBm
Frequency 2 = 440 Hz at –19 dBm
```

- IP: indirizzo IPv4 sotto forma di x.x.x. x, dove x è compreso tra 0 e 255. Esempio: 10.1.2.100.
- ID utente: l'ID utente viene visualizzato in un URL; fino a 63 caratteri.
- Telefono: una stringa di numero di telefono, ad esempio, 14081234567 * 69, * 72, 345678; o un URL generico, ad esempio 1234@10.10.10.100:5068 o jsmith@Cisco.com. La stringa può contenere fino a un massimo di 39 caratteri.
- PhTmplt: un modello di numero di telefono. Ogni modello può contenere uno o più percorsi che sono separati da una virgola (,). Lo spazio vuoto all'inizio di ogni modello viene ignorato. "?" e "*" rappresentano i caratteri jolly. Per rappresentare effettivamente, utilizzare %xx. Ad esempio, %2a rappresenta *. Il modello può contenere fino a un massimo di 39 caratteri. Esempi: "1408*, 1510*", "1408123????, 555?1.".
- Porta: il numero di porta TCP/UDP (0-65535). È possibile specificare in formato decimale o esadecimale.
- ProvisioningRuleSyntax: script sintassi utilizzata per definire le regole di risincronizzazione di configurazione e di aggiornamento del firmware.
- PwrLevel: livello di potenza espresso in dBm con una posizione decimale, ad esempio –13,5 o 1,5 (dBm).
- RscTmplt: un modello di codice di stato risposta SIP, come ad esempio "404, 5*", “61?”, "407, 408, 487, 481". Può contenere un massimo di 39 caratteri.
- Sig<n>: valore di n bit di stato di accesso effettuato. È possibile specificare in formato decimale o esadecimale. Un simbolo "-" deve precedere i valori negativi. Un simbolo + prima di valori positivi è facoltativo.
- Codici con asterisco: codice di attivazione di un servizio supplementare, come ad esempio * 69. Il codice può contenere fino a un massimo di 7 caratteri.
- Str<n>: una stringa generica con un massimo di n caratteri non riservati.
- Time<n>: tempo di durata in secondi, con fino a n posizioni decimali. I punti decimali addizionali vengono ignorati.
- ToneScript: un miniscript che consente di specificare i parametri di frequenza, livello e cadenza di un segnale di chiamata in corso. Lo script può contenere fino a 127 caratteri.

Syntax: FreqScript;Z_1[;Z_2].

La sezione Z_1 è simile alla sezione S_1 in un CadScript, fatta eccezione per il fatto che ogni segmento on/off è seguito da un parametro di componenti della frequenza: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}[,on_{i,3}/off_{i,3}/f_{i,3}[,on_{i,4}/off_{i,4}/f_{i,4}[,on_{i,5}/off_{i,5}/f_{i,5}[,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ dove:

- $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
- $1 < n_k < 6$ specifica i componenti della frequenza nel FreqScript utilizzati in questo segmento.

Se più di un componente frequenza viene utilizzato in un segmento, i componenti vengono sommati insieme.

Esempio 1 - Segnale di linea:

```
350@-19,440@-19;10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 10s
```

Esempio 2 - Segnale acustico intermittente:

```
350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 12s
```

- Uns<n>: valore di n bit senza segno, dove n = 8, 16 o 32. È possibile specificare in formato decimale o esadecimale, ad esempio 12 o 0x18, a condizione che il valore possa essere contenuto in n bit.

Nota Tenere presente quanto segue:

- < Nome par> rappresenta il nome di un parametro di configurazione. In un profilo, il tag corrispondente è formato sostituendo lo spazio con un carattere con trattini bassi "_", come ad esempio **Par_Name**.
- Un campo di valore predefinito vuoto indica una stringa vuota < "" >.
- Il telefono continua a utilizzare gli ultimi valori configurati per i tag che non sono presenti in un determinato profilo.
- I modelli vengono confrontati nell'ordine specificato. Viene selezionata la prima corrispondenza e *non la più vicina*. Il nome del parametro deve corrispondere esattamente.
- Se viene assegnata a un profilo più di una definizione per un parametro, l'ultima in tale definizione nel file è quella che ha effetto nel telefono.
- Una specifica del parametro con un valore di parametro vuoto forza il parametro al suo valore predefinito. Per specificare una stringa vuota, invece, utilizzare una stringa vuota "" come valore del parametro.

Aggiornamenti del profilo e del firmware

Il telefono supporta il provisioning remoto protetto (configurazione) e gli aggiornamenti del firmware. Un telefono non dotato di provisioning può ricevere un profilo crittografato destinato a tale dispositivo. Il telefono non richiede una chiave esplicita grazie a un meccanismo di primo provisioning protetto che utilizza la funzionalità SSL.

Per avviare o completare un aggiornamento del profilo, per aggiornare il firmware o se sono necessari aggiornamenti intermedi per raggiungere uno stato di aggiornamento futuro da una versione precedente, non è necessario l'intervento dell'utente. Una risincronizzazione del profilo viene tentata solo quando il telefono è inattivo, in quanto una risincronizzazione può attivare un riavvio software e interrompere una chiamata.

I parametri con scopi generici gestiscono il processo di provisioning. Ciascun telefono può essere configurato in modo da contattare periodicamente un server di provisioning normale (criteri). La comunicazione con l'NPS non richiede l'uso di un protocollo sicuro perché il profilo aggiornato viene crittografato utilizzando una chiave segreta condivisa. NPS può essere un server TFTP, HTTP o HTTPS standard con certificati client.

L'amministratore può eseguire l'aggiornamento, riavviare il sistema, riavviare o risincronizzare i telefoni tramite l'interfaccia utente basata su Web del telefono. L'amministratore può anche eseguire queste attività mediante un messaggio di notifica SIP.

I profili di configurazione sono generati utilizzando gli strumenti comuni open source che si integrano con sistemi di provisioning del provider di servizi.

Argomenti correlati

Consentire e configurare gli aggiornamenti del profilo, a pagina 37

Consentire e configurare gli aggiornamenti del profilo

Gli aggiornamenti del profilo possono essere consentiti a intervalli specifici. I profili aggiornati vengono inviati da un server al telefono tramite TFTP, HTTP o HTTPS.

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Selezionare **Voice** > **Provisioning**.

Passaggio 2 Nella sezione **Configuration Profile**, scegliere **Yes** dalla casella di riepilogo a discesa **Provision Enable**.

Passaggio 3 Immettere i parametri.

Passaggio 4 Fare clic su **Submit All Changes**.

Argomenti correlati

Aggiornamenti del profilo e del firmware, a pagina 37

Consentire e configurare gli aggiornamenti del firmware

Gli aggiornamenti del firmware possono essere consentiti a intervalli specifici. Il firmware aggiornato viene inviato da un server al telefono tramite TFTP, HTTP o HTTPS. La sicurezza non è un problema con un aggiornamento del firmware perché il firmware non contiene dati personali.

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Selezionare **Voice** > **Provisioning**.

Passaggio 2 Nella sezione **Firmware Upgrade** scegliere **Yes** dalla casella di riepilogo a discesa **Upgrade Enable**.

Passaggio 3 Immettere i parametri.

Passaggio 4 Fare clic su **Submit All Changes**.

Aggiornamento del firmware tramite TFTP, HTTP o HTTPS

Il telefono supporta l'aggiornamento di immagini singole tramite TFTP, HTTP o HTTPS.

Nota Il downgrade alle versioni precedenti potrebbe non essere disponibile per tutti i dispositivi. Per ulteriori informazioni, consultare le note sulla versione per il telefono e la versione del firmware in uso.

Prima di iniziare

Il file di caricamento del firmware deve essere scaricato su un server accessibile.

Procedura

Passaggio 1 Rinominare l'immagine nel modo seguente:

da **cp-x8xx-sip.aa-b-cMPP.cop** a **cp-x8xx-sip.aa-b-cMPP.tar.gz**

dove:

x8xx è la serie del telefono, ad esempio 6841.

aa-b-c è il numero di versione, ad esempio 10-4-1

Passaggio 2 Utilizzare il comando **tar – xzvf** per eseguire l'untar del tarball.

Passaggio 3 Copiare la cartella in una directory di download TFTP, HTTP o HTTPS.

Passaggio 4 Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Passaggio 5 Selezionare **Voice** > **Provisioning**.

Passaggio 6 Trovare il nome del file di caricamento che termina con **.loads** e aggiungerlo all'URL valido.

Passaggio 7 Fare clic su **Submit All Changes**.

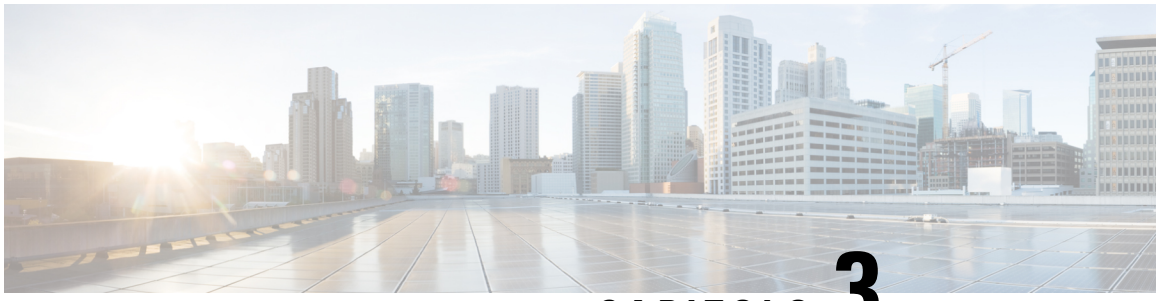
Aggiornamento del firmware con un comando di browser

Un comando di aggiornamento immesso nella barra degli indirizzi del browser può essere utilizzato per eseguire l'aggiornamento del firmware su un telefono. Il telefono viene aggiornato solo quando è inattivo. L'aggiornamento viene eseguito automaticamente una volta completata la chiamata.

Procedura

Per aggiornare il telefono con un URL in un browser Web, immettere il seguente comando:

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```



CAPITOLO 3

Server di preprovisioning e provisioning interni

Server di preprovisioning e provisioning interni

Il provider di servizi esegue il preprovisioning dei telefoni, diversi dalle unità RC, con un profilo. Il profilo di preprovisioning può comprendere una serie limitata di parametri che risincronizza il telefono. Il profilo può comprendere anche una serie completa di parametri offerti dal server remoto. Per impostazione predefinita, il telefono si risincronizza all'accensione e a intervalli configurati nel profilo. Quando l'utente si connette al telefono presso la sede del cliente, il dispositivo scarica il profilo aggiornato ed eventuali aggiornamenti firmware.

Questo processo di preprovisioning, distribuzione e provisioning remoto può essere eseguito in diversi modi.

Preparazione del server e strumenti software

Gli esempi in questo capitolo richiedono la disponibilità di uno o più server. Questi server possono essere installati ed eseguiti su un PC locale:

- TFTP (UDP porta 69)
- syslog (UDP porta 514)
- HTTP (porta TCP 80)
- HTTPS (porta TCP 443).

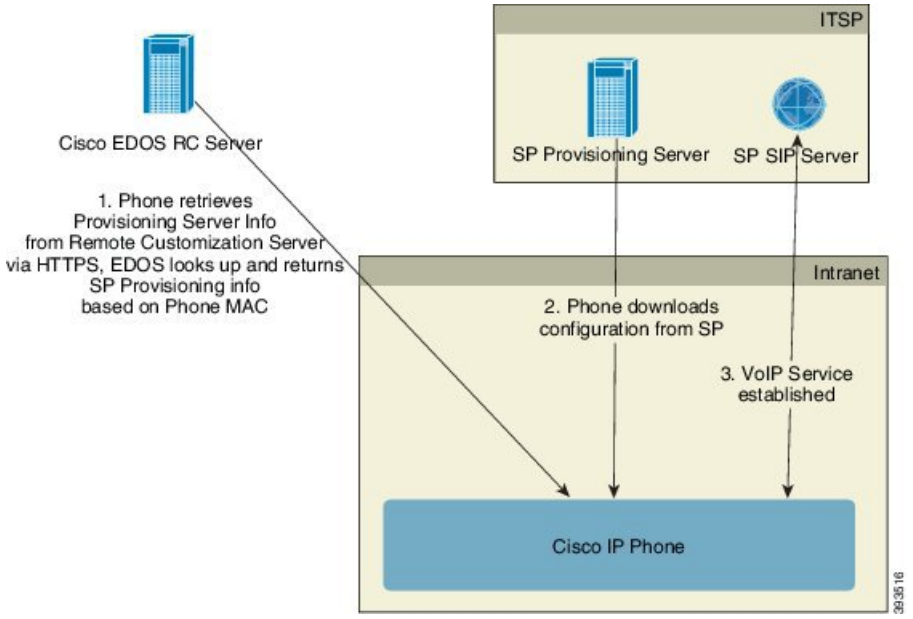
Per risolvere i problemi di configurazione del server, è utile installare client per ogni tipo di server in un computer server separato. In questo modo viene definita il corretto funzionamento del server, indipendentemente dall'interazione con i telefoni.

Si consiglia inoltre di installare i seguenti strumenti software:

- Per generare profili di configurazione, installare l'utilità di compressione gzip open source.

- Per la crittografia del profilo e le operazioni HTTPS, installare il pacchetto software OpenSSL open source.
- Per verificare la generazione di profili dinamici e il provisioning remoto in un unico passaggio tramite HTTPS, è consigliabile un linguaggio di scripting con supporto di scripting CGI. Gli strumenti del linguaggio Perl open source sono un esempio di tale linguaggio di scripting.
- Per verificare scambi protetti tra i server di provisioning e i telefoni, installare un programma di monitoraggio di pacchetti Ethernet (ad esempio, Ethereal/Wireshark scaricabile gratuitamente). Acquisire una traccia di pacchetti Ethernet dell'interazione tra il telefono e il server di provisioning. A tale scopo, eseguire il programma di monitoraggio di pacchetti su un PC connesso a uno switch con il mirroring porta abilitato. Per le transazioni HTTPS, è possibile utilizzare l'utilità ssldump.

Distribuzione della personalizzazione remota (RC)



Tutti i telefoni contattano il server Cisco EDOS RC fino a quando non viene eseguito il provisioning inizialmente.

In un modello di distribuzione RC, un cliente acquista un telefono che è già stato associato a un provider di servizi specifico nel server Cisco EDOS RC. Il provider di servizi di telefonia Internet (ITSP) imposta e gestisce un server di provisioning e registra le informazioni del server di provisioning sul server Cisco EDOS RC.

Quando il telefono è acceso con una connessione a Internet, lo stato di personalizzazione del telefono senza provisioning è **aperto**. Innanzitutto, il telefono contatta il server DHCP locale per informazioni sul server di provisioning e imposta lo stato di personalizzazione del telefono. Se l'interruzione del DHCP viene eseguita correttamente, lo stato di personalizzazione è impostato su **Annullato** e l'RC non viene tentato poiché il DHCP ha fornito le informazioni necessarie sul server di provisioning.

Quando un telefono si connette a una rete per la prima volta o dopo un ripristino delle impostazioni di fabbrica, se non sono presenti opzioni DHCP, contatta un server di attivazione del dispositivo per il provisioning zero touch. I nuovi telefoni utilizzeranno «activate.cisco.com» anziché «webapps.cisco.com» per il provisioning.

I telefoni con una versione del firmware precedente alle 11.2(1) continueranno a utilizzare webapps.cisco.com. Cisco consiglia di consentire l'utilizzo di entrambi i nomi di dominio tramite il firewall.

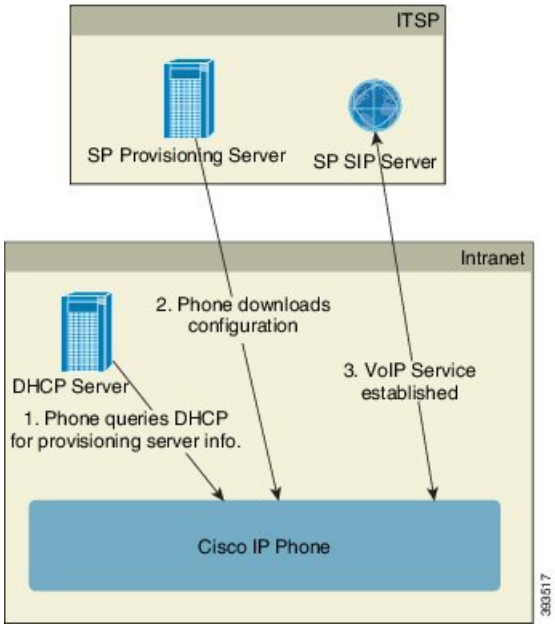
Se il server DHCP non fornisce le informazioni sul server di provisioning, il telefono contatta il server Cisco EDOS RC e fornisce il relativo indirizzo MAC e modello e lo stato di personalizzazione viene impostato su **In sospeso**. Il server Cisco EDOS risponde con il le informazioni associate del server di provisioning del provider di servizi, tra cui l'URL del server di provisioning e lo stato di personalizzazione del telefono è impostato su **In attesa di personalizzazione**. Il telefono quindi esegue un comando URL di risincronizzazione per ripristinare la configurazione del provider di servizi e, se va a buon fine, lo stato di personalizzazione è impostato su **Acquisito**.

Se il server Cisco EDOS RC non dispone di un provider di servizi associato con il telefono IP Cisco, lo stato di personalizzazione del telefono è impostato su **Non disponibile**. Il telefono può essere configurato manualmente o può essere aggiunta un'associazione per il provider di servizi del telefono sul server Cisco EDOS.

Se viene eseguito il provisioning di un telefono tramite LCD o utilità di configurazione Web, prima che lo stato di personalizzazione diventi **Acquisito**, lo stato di personalizzazione è impostato su **Interrotto** e il server Cisco EDOS non verrà interrogato a meno che non venga eseguito il ripristino delle impostazioni di fabbrica del telefono.

Una volta eseguito il provisioning del telefono, il server Cisco EDOS RC non viene utilizzato a meno che non viene eseguito il ripristino delle impostazioni di fabbrica del telefono.

Preprovisioning del dispositivo interno



Con la configurazione predefinita di fabbrica Cisco, il telefono tenta automaticamente di risincronizzarsi con un profilo su un server TFTP. Un server DHCP gestito su una rete LAN fornisce le informazioni sul profilo e sul server TFTP configurato per il preprovisioning sul dispositivo. Il provider di servizi connette ogni nuovo telefono alla LAN. Il telefono si risincronizza automaticamente al server TFTP locale e inizializza il proprio stato interno in preparazione della distribuzione. In genere, questo profilo preprovisioning include l'URL di

un server di provisioning remoto. Il server di provisioning mantiene il dispositivo aggiornato dopo che il dispositivo viene distribuito e connesso alla rete del cliente.

Il codice a barre del dispositivo sottoposto a preprovisioning può essere scansionato per registrare il relativo indirizzo MAC o numero di serie prima che il telefono venga spedito al cliente. Queste informazioni possono essere utilizzate per creare il profilo da cui il telefono si risincronizza.

Quando riceve il telefono, il cliente lo connette al collegamento a banda larga. All'accensione, il telefono contatta il server di provisioning mediante l'URL configurato durante il preprovisioning. Il telefono in questo modo può risincronizzarsi e aggiornare il profilo e il firmware in base alle necessità.

Argomenti correlati

Distribuzione al dettaglio, a pagina 6
Provisioning su TFTP, a pagina 44

Impostazione del server di provisioning

In questa sezione vengono descritti i requisiti di impostazione per il provisioning di un telefono utilizzando diversi server e scenari. Ai fini di questo documento e per il test, i server di provisioning vengono installati ed eseguiti su un PC locale. Inoltre, strumenti software generalmente disponibili sono utili per il provisioning dei telefoni.

Provisioning su TFTP

I telefoni supportano TFTP per la risincronizzazione del provisioning e le operazioni di aggiornamento del firmware. Quando i dispositivi vengono distribuiti in remoto, è consigliabile utilizzare HTTPS, ma possono anche essere utilizzati HTTP e TFTP. Quindi richiede la crittografia dei file di provisioning per aggiungere protezione, poiché offre maggiore affidabilità, meccanismi NAT e di protezione router dati. TFTP è utile per il preprovisioning interno di un numero elevato di dispositivi senza provisioning.

Il telefono è in grado di ottenere un indirizzo IP del server TFTP direttamente dal server DHCP tramite l'opzione 66 DHCP. Se è configurata una Profile_Rule con il percorso del file di tale server TFTP, il dispositivo scarica il suo profilo dal server TFTP. Il download si verifica quando il dispositivo è connesso a una rete LAN e acceso.

La Profile_Rule fornita con la configurazione predefinita di fabbrica è *&PN*.cfg, dove *&PN* rappresenta il nome del modello di telefono.

Ad esempio, per un CP-6841-3PCC, il nome file è CP-6841-3PCC.cfg.

Per un dispositivo con il profilo predefinito di fabbrica, all'accensione, il dispositivo si risincronizza con questo file sul server TFTP locale che specifica l'opzione 66 DHCP. Il percorso file è relativo alla directory root virtuale del server TFTP.

Argomenti correlati

Preprovisioning del dispositivo interno, a pagina 43

Controllo endpoint remoto e NAT

Il telefono è compatibile con il servizio NAT (Network Address Translation) per accedere a Internet tramite un router. Per maggiore sicurezza, il router potrebbe tentare di bloccare pacchetti in arrivo non autorizzati mediante l'implementazione di NAT simmetrico, una strategia di filtraggio dei pacchetti che limita

rigorosamente i pacchetti ai quali è consentito l'accesso alla rete protetta da Internet. Per questo motivo, il provisioning remoto tramite TFTP non è consigliato.

Il VoIP può coesistere con NAT solo quando viene fornita una qualche forma di attraversamento NAT. Configurare l'attraversamento semplice di UDP attraverso NAT (STUN). Questa opzione richiede che l'utente:

- Abbia un indirizzo IP dinamico esterno (pubblico) dal proprio servizio
- Abbia un computer che esegue il software del server STUN
- Abbia un dispositivo periferico con un meccanismo NAT asimmetrico

Provisioning su HTTP

Il telefono si comporta come un browser che richiede pagine Web da un sito remoto in Internet. Ciò offre un mezzo affidabile per raggiungere il server di provisioning, anche quando un router del cliente implementa il NAT simmetrico o altri meccanismi di protezione. HTTP e HTTPS funzionano in modo più affidabile di TFTP in distribuzioni remote, in particolare quando le unità distribuite sono connesse dietro firewall residenziali o router abilitati per NAT. HTTP e HTTPs vengono utilizzati alternativamente nelle seguenti descrizioni di tipo di richiesta.

Il provisioning di base basato su HTTP si basa sul metodo HTTP GET per ripristinare i profili di configurazione. In genere, viene creato un file di configurazione per ciascun telefono distribuito e questi file vengono memorizzati in una directory server HTTP. Quando il server riceve la richiesta GET, restituisce semplicemente il file specificato nell'intestazione della richiesta GET.

Invece di un profilo statico, il profilo di configurazione può essere generato in modo dinamico interrogando il database di un cliente e producendo il profilo al volo.

Quando il telefono richiede una risincronizzazione, può utilizzare il metodo HTTP POST per richiedere i dati di configurazione della risincronizzazione. Il dispositivo può essere configurato per trasmettere determinate informazioni di stato e identificazione al server all'interno del corpo della richiesta HTTP POST. Il server utilizza tali informazioni per generare un profilo di configurazione della risposta desiderato o per memorizzare le informazioni di stato per l'analisi e il monitoraggio successivi.

Come parte delle richieste GET e POST, il telefono include automaticamente le informazioni di identificazione di base nel campo Agente utente dell'intestazione della richiesta. Queste informazioni includono il produttore, il nome del prodotto, la versione del firmware corrente e il numero di serie del dispositivo.

Nell'esempio seguente è riportato il campo della richiesta Agente utente da un CP-6841-3PCC:

```
User-Agent: Cisco-CP-6841-3PCC/11.0 (00562b043615)
```

Quando il telefono viene configurato in modo da risincronizzarsi con un profilo di configurazione tramite HTTP, si consiglia di utilizzare HTTPS oppure di crittografare il profilo per proteggere le informazioni riservate. I profili crittografati che il telefono scarica tramite HTTP evitano il pericolo di esposizione di informazioni riservate contenute nel profilo di configurazione. Questa modalità di risincronizzazione produce un carico di calcolo inferiore sul server di provisioning rispetto a quello generato con l'utilizzo di HTTPS.

Il telefono può decrittografare i profili con uno dei seguenti metodi di crittografia:

- Crittografia AES-256-CBC
- Crittografia basata su RFC 8188 con cifratura AES-128-GCM

Nota I telefoni supportano HTTP versione 1.0, HTTP versione 1.1 e codifica in chunk quando HTTP versione 1.1 è il protocollo di trasporto negoziato.

Gestione codice di stato HTTP per risincronizzazione e aggiornamento

Il telefono supporta la risposta HTTP per il provisioning remoto (risincronizzazione). Il comportamento del telefono corrente è suddiviso in tre modi:

- A: riuscito, in cui i valori "Risincronizzazione periodica" e "Ritardo casuale risincronizzazione" determinano richieste successive.
- B: errore quando File non trovato o profilo danneggiato. Il valore "Risincronizzazione ritardo nuovo tentativo da errore" determina le richieste successive.
- C: altri errori quando un indirizzo IP o URL non valido genera un errore di connessione. Il valore "Risincronizzazione ritardo nuovo tentativo da errore" determina le richieste successive.

Tabella 2: Comportamento del telefono per le risposte HTTP

Codice di stato HTTP	Descrizione	Comportamento del telefono
301 Spostato in modo permanente	Queste richiesta e quelle future devono essere indirizzate a una nuova posizione.	Riprovare richiesta immediatamente con una nuova posizione.
302 Trovato	Noto come temporaneamente spostato.	Riprovare richiesta immediatamente con una nuova posizione.
3xx	Altre risposte 3xx non elaborate.	C
400 Richiesta non valida	Non è possibile soddisfare la richiesta a causa di sintassi non valida.	C
401 Non autorizzato	Sfida di autenticazione di accesso di base o digest.	Riprovare a effettuare immediatamente la richiesta con le credenziali di autenticazione. Numero massimo di 2 tentativi. In caso di errore, il comportamento del telefono è C.
403 Non consentito	Il server rifiuta di rispondere.	C
404 Non trovato	Risorsa richiesta non trovata. Le richieste successive dal client sono consentite.	B
407 Autenticazione del proxy richiesta	Sfida di autenticazione di accesso di base o digest.	Riprovare a effettuare immediatamente la richiesta con le credenziali di autenticazione. Numero massimo di due tentativi. In caso di errore, il comportamento del telefono è C.

Codice di stato HTTP	Descrizione	Comportamento del telefono
4xx	Altri codici di stato di errore client non vengono elaborati.	C
500 Errore server interno	Messaggio di errore generico.	Il comportamento del telefono è C.
501 Non implementato	Il server non riconosce il metodo di richiesta o non esiste la possibilità di soddisfare la richiesta.	Il comportamento del telefono è C.
502 Gateway non valido	Il server funge da gateway o proxy e riceve una risposta non valida dal server upstream.	Il comportamento del telefono è C.
503 Servizio non disponibile	Il server non è attualmente disponibile (sovraccaricato o inattivo per la manutenzione). Si tratta di uno stato temporaneo.	Il comportamento del telefono è C.
504 Timeout gateway	Il server funge da gateway o proxy e non riceve una risposta valida dal server upstream.	C
5xx	Altro errore del server	C

Provisioning su HTTPS

Per una maggiore sicurezza nella gestione remota delle unità distribuite, il telefono supporta HTTPS per il provisioning. Ogni telefono ha un certificato Client SLL univoco e la chiave privata associata, oltre a un certificato principale del server Sipura CA. Consente al telefono di riconoscere i server di provisioning autorizzati e rifiutare quelli non autorizzati. Al contrario, il certificato client consente al server di provisioning di identificare il singolo dispositivo che invia la richiesta.

Affinché un provider di servizi gestisca la distribuzione tramite HTTPS, è necessario generare un certificato del server per ciascun server di provisioning con cui un telefono si risincronizza utilizzando HTTPS. Il certificato del server deve essere firmato dalla chiave principale dell'autorità di certificazione dei server Cisco, certificato che posseggono tutte le unità distribuite. Per ottenere un certificato del server firmato, il provider di servizi deve inoltrare una richiesta a Cisco, che accede e restituisce il certificato del server per l'installazione sul server di provisioning.

Il certificato del server di provisioning deve contenere il campo nome comune (CN) e il nome di dominio completo dell'host del server in esecuzione nell'oggetto. Se lo si desidera, può contenere informazioni dopo l'host FQDN, separate da un carattere barra (/). Negli esempi seguenti vi sono delle voci CN accettate come valide dal telefono:

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

Oltre a verificare il certificato del server, il telefono testa l'indirizzo IP del server rispetto a una ricerca DNS del nome del server specificato nel certificato del server.

Come ottenere un certificato del server firmato

L'utilità OpenSSL può generare una richiesta di firma del certificato. L'esempio seguente mostra il comando **openssl** che produce una coppia di chiavi pubblica/privata RSA a 1024 bit e una richiesta di forma del certificato:

```
openssl req -new -out provserver.csr
```

Questo comando genera la chiave privata del server in **privkey.pem** e una richiesta di firma del certificato corrispondente in **provserver.csr**. Il provider di servizi mantiene il segreto **privkey.pem** e invia **provserver.csr** a Cisco per a firma. Alla ricezione del file **provserver.csr**, Cisco genera **provserver.crt**, il certificato del server firmato.

Procedura

Passaggio 1 Accedere a https://software.cisco.com/software/cda/home ed eseguire la connessione con le proprie credenziali CCO.

Nota Quando un telefono si connette a una rete per la prima volta o dopo un ripristino delle impostazioni di fabbrica e non sono presenti opzioni DHCP, contatta un server di attivazione del dispositivo per il provisioning zero touch. I nuovi telefoni utilizzano «activate.cisco.com» anziché «webapps.cisco.com» per il provisioning. I telefoni con una versione del firmware precedente alle 11.2(1) continuano a utilizzare «webapps.cisco.com». Si consiglia di consentire l'utilizzo di entrambi i nomi di dominio tramite il firewall.

Passaggio 2 Selezionare **Gestione certificati**.

Nella scheda **Firma CSR**, viene caricato per la firma il CSR della fase precedente.

Passaggio 3 Dalla casella di riepilogo a discesa **Seleziona prodotto**, selezionare il **firmware SPA1xx 1.3.3 e i più recenti firmware /SPA232D 1.3.3, /SPA5xx 7.5.6 e /CP-78xx-3PCC/CP-88xx-3PCC**.

Nota Questo prodotto include i telefoni multipiattaforma Cisco IP Phone serie 6800.

Passaggio 4 Nel campo **File CSR**, fare clic su **Sfoglia** e selezionare il CSR da firmare.

Passaggio 5 Selezionare il metodo di crittografia:

- MD5
- SHA1
- SHA256

Cisco consiglia di selezionare la crittografia SHA256.

Passaggio 6 Dalla casella di riepilogo a discesa **Durata firma**, selezionare la durata applicabile (ad esempio, 1 anno).

Passaggio 7 Fare clic su **Richiesta di firma certificato**.

Passaggio 8 Selezionare una delle seguenti opzioni per ricevere il certificato firmato:

- **Immettere indirizzo e-mail del destinatario**: se si desidera ricevere il certificato via e-mail, immettere l'indirizzo e-mail in questo campo.
- **Download**: se si desidera scaricare il certificato firmato fare clic su questa opzione.

Passaggio 9 Fare clic su **Submit**.

Il certificato del server firmato viene inviato tramite e-mail all'indirizzo precedentemente fornito o scaricato.

Certificato principale client CA del telefono multipiattaforma

Cisco fornisce inoltre al provider di servizi un certificato principale client del telefono multipiattaforma. Questo certificato di origine certifica l'autenticità del certificato client che ogni telefono ha. I telefoni multipiattaforma supportano anche certificati firmati di terze parti, come quelli forniti da Verisign, Cybertrust e così via.

Il certificato client unico che ogni dispositivo offre durante una sessione HTTPS contiene l'identificazione delle informazioni incorporate nel relativo campo di oggetto. Queste informazioni possono essere rese disponibili dal server HTTPS a uno script CGI richiamato per gestire le richieste protette. In particolare, l'oggetto del certificato indica il nome del prodotto unitario (elemento OU), l'indirizzo MAC (elemento S) e il numero di serie (elemento L).

L'esempio riportato di seguito dal campo del certificato client dei telefoni multipiattaforma Cisco IP Phone 6841 mostra i seguenti elementi:

```
OU=CP-6841-3PCC, L=88012BA01234, S=000e08abcdef
```

Per determinare se un telefono ha un certificato individualizzato, utilizzare la variabile macro di provisioning $CCERT. Il valore della variabile si estende a quello Installato o Non installato, in base alla presenza o all'assenza di un certificato client unico. Nel caso di un certificato generico, è possibile ottenere il numero di serie dell'unità dall'intestazione HTTP richiesta nel campo User-Agent.

I server HTTPS possono essere configurati per richiedere certificati SSL dai client di connessione. Se abilitato, il server può utilizzare il certificato principale client del telefono multipiattaforma fornito da Cisco per verificare il certificato client. Il server può quindi fornire le informazioni del certificato a un CGI per ulteriori elaborazioni.

La posizione per l'archiviazione dei certificati può variare. Ad esempio, in un'installazione Apache, i percorsi di file per l'archiviazione del certificato firmato di provisioning, la chiave privata associata e il certificato client principale CA del telefono multipiattaforma sono i seguenti:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

Per informazioni specifiche, fare riferimento alla documentazione di un server HTTPS.

L'autorità della chiave del certificato client Cisco firma ogni certificato univoco. Il certificato principale corrispondente viene messo a disposizione dei provider di servizi per scopi di autenticazione client.

Server di provisioning ridondanti

Il server di provisioning può essere specificato come un indirizzo IP o come un nome di dominio completo (FQDN). L'utilizzo di un FQDN facilita la distribuzione di server di provisioning ridondanti. Quando il server di provisioning è identificato tramite un FQDN, il telefono tenta di risolvere l'FQDN su un indirizzo IP tramite DNS. Solo i record DNS A sono supportati per il provisioning; la risoluzione dell'indirizzo DNS SRV non è

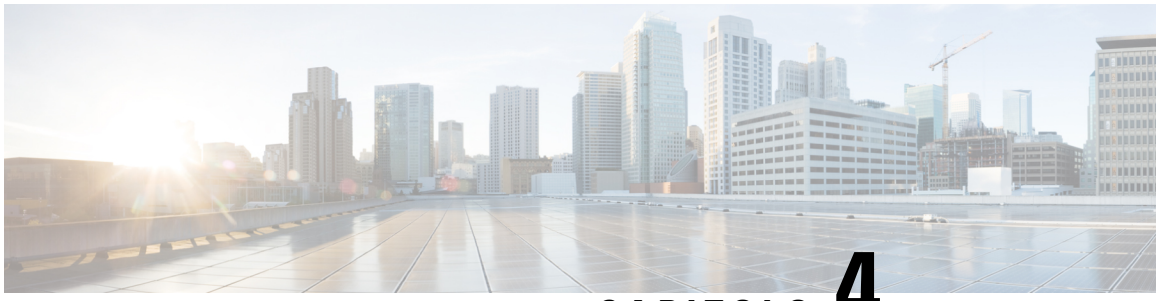
disponibile per il provisioning. Il telefono continua a elaborare i record A fino a che il server risponde. Se nessun server associato ai record A risponde, il telefono registra un errore sul server syslog.

Syslog Server

Se un server syslog è configurato su il telefono tramite l'utilizzo dei parametri <Syslog Server>, le operazioni di risincronizzazione e di aggiornamento inviano messaggi al server syslog. Un messaggio può essere generato all'inizio di una richiesta di file remoto (profilo di configurazione o carico del firmware) e alla conclusione dell'operazione (indicando il successo o il fallimento).

I messaggi registrati vengono configurati nei parametri e nelle macro seguenti estesi nei messaggi di syslog effettivi:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



CAPITOLO 4

Esempi di provisioning

Panoramica degli esempi di provisioning

In questo capitolo vengono descritte le procedure di esempio per il trasferimento dei profili di configurazione tra il telefono e il server di provisioning.

Per informazioni sulla creazione di profili di configurazione, consultare Formati di provisioning, a pagina 15.

Risincronizzazione di base

In questa sezione viene illustrata le funzionalità di risincronizzazione di base dei telefoni.

Risincronizzazione di TFTP

Il telefono supporta più protocolli di rete per il ripristino dei profili di configurazione. Il protocollo di trasferimento del profilo di base è TFTP (RFC1350). TFTP è molto utilizzato per il provisioning di dispositivi di rete all'interno di reti LAN private. Anche se non è consigliato per la distribuzione di endpoint remoti su Internet, TFTP può essere utile per la distribuzione all'interno di aziende di piccole dimensioni, per il preprovisioning interno e per lo sviluppo e i test. Vedere Preprovisioning del dispositivo interno, a pagina 43 per ulteriori informazioni sul prepositioning interno. Nella seguente procedura, un profilo è stato modificato dopo il download di un file da un server TFTP.

Procedura

Passaggio 1 All'interno di un ambiente LAN, collegare un PC e telefono a un hub, switch o router piccolo.

Passaggio 2 Sul PC installare e attivare un server TFTP.

Passaggio 3 Utilizzare un editor di testo per creare un profilo di configurazione che consente di impostare il valore per GPP_A pari a 12345678 come mostrato nell'esempio.

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

Passaggio 4 Salvare il profilo con il nome `basic.txt` nella directory principale del server TFTP.

È possibile verificare che il server TFTP sia configurato correttamente: richiedere il file `basic.txt` utilizzando un client TFTP diverso dal telefono. Di preferenza, utilizzare un client TFTP che sia in esecuzione su un host separato dal server di provisioning.

Passaggio 5 Aprire il browser Web del PC nella pagina di configurazione admin/advanced. Ad esempio, se l'indirizzo IP del telefono è 192.168.1.100:

```
http://192.168.1.100/admin/advanced
```

Passaggio 6 Selezionare la scheda **Voice** > **Provisioning** e controllare i valori dei parametri per scopi generici da GPP_A a GPP_P. Questi devono essere vuoti.

Passaggio 7 Risincronizzare il telefono del test sul profilo di configurazione `basic.txt` aprendo l'URL di risincronizzazione in una finestra del browser Web.

Se l'indirizzo IP del server TFTP è 192.168.1.200, il comando deve essere simile al seguente esempio:

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

Quando il telefono riceve questo comando, il dispositivo all'indirizzo 192.168.1.100 richiede il file `basic.txt` dal server TFTP all'indirizzo IP 192.168.1.200. Quindi il telefono analizza il file scaricato e aggiorna il parametro GPP_A con il valore 12345678.

Passaggio 8 Verificare che il parametro sia stato aggiornato correttamente: aggiornare la pagina di configurazione nel browser Web del PC e selezionare la scheda **Voice** > **Provisioning**.

A questo punto il parametro GPP_A deve contenere il valore 12345678.

Utilizzo di syslog per registrare i messaggi

Il telefono invia un messaggio di syslog al server syslog designato quando il dispositivo sta per risincronizzarsi su un server di provisioning e dopo aver completato positivamente o negativamente la risincronizzazione (riuscita o errore). Per identificare il server, è possibile accedere alla pagina web di amministrazione del telefono (vedere Accesso alla pagina Web del telefono, a pagina 9), selezionare **Voice** > **System** e identificare il server nel parametro **Syslog_Server** della sezione **Optional Network Configuration**. Configurare l'indirizzo IP del server syslog nel dispositivo e osservare i messaggi che vengono generati durante le rimanenti procedure.

Procedura

Passaggio 1 Installare e attivare un server syslog sul PC locale.

Passaggio 2 Programmare l'indirizzo IP del PC nel parametro Syslog_Server del profilo e inviare la modifica:

```
<Syslog_Server>192.168.1.210</Syslog_Server>
```

Passaggio 3 Fare clic sulla scheda **System** e immettere il valore del server syslog locale nel parametro Syslog_Server.

Passaggio 4 Ripetere l'operazione di risincronizzazione come descritto in Risincronizzazione di TFTP, a pagina 51.

Il dispositivo genera due messaggi di syslog durante la risincronizzazione. Il primo messaggio indica che una richiesta è in corso. Il secondo messaggio contrassegna lo stato della risincronizzazione (riuscita o errore).

Passaggio 5 Verificare che il server syslog abbia ricevuto messaggi analoghi ai seguenti:

```
CP-68xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txtc.txt
```

Messaggi dettagliati sono disponibili programmando un parametro Debug_Server (invece del parametro Syslog_Server) con l'indirizzo IP del server syslog e impostando Debug_Level su un valore compreso tra 0 e 3 (essendo 3 il più dettagliato):

```
<Debug_Server>192.168.1.210</Debug_Server>
<Debug_Level>3</Debug_Level>
```

È possibile configurare i contenuti di tali messaggi utilizzando i seguenti parametri:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Se uno di questi parametri viene cancellato, il corrispondente messaggio di syslog non viene generato.

Risincronizzazione automatica di un dispositivo

Un dispositivo può eseguire periodicamente la risincronizzazione al server di provisioning per garantire che eventuali modifiche del profilo apportate sul server vengono propagate al dispositivo endpoint (in alternativa all'invio di una richiesta di risincronizzazione esplicita all'endpoint).

Per fare in modo che il telefono si risincronizzi periodicamente su un server, viene definito un URL del profilo di configurazione utilizzando il parametro Profile_Rule e viene definito un periodo di risincronizzazione utilizzando il parametro Resync_Periodic.

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Selezionare **Voice** > **Provisioning**.

Passaggio 2 Definire il parametro Profile_Rule. Questo esempio presuppone un indirizzo IP del server TFTP uguale a 192.168.1.200.

Passaggio 3 Nel campo **Resync Periodic**, immettere un valore piccolo per il test, come ad esempio **30** secondi.

Passaggio 4 Fare clic su **Submit All Changes**.

Grazie alle nuove impostazioni dei parametri, il telefono si risincronizza due volte al minuto al file di configurazione specificato dall'URL.

Passaggio 5 Osservare i messaggi ricevuti nella traccia syslog (come descritto nella sezione Utilizzo di syslog per registrare i messaggi, a pagina 52).

Passaggio 6 Assicurarsi che il campo **Resync On Reset** sia impostato su **Yes**.

```
<Resync_On_Reset>Yes</Resync_On_Reset>
```

Passaggio 7 Spegnere e riaccendere il telefono per forzare la risincronizzazione sul server di provisioning.

Se l'operazione di risincronizzazione ha esito negativo per qualsiasi motivo, come ad esempio se il server non risponde, l'unità attende (per il numero di secondi configurato in **Resync Error Retry Delay**) prima che tenti nuovamente la risincronizzazione. Se **Ritardo nuovo tentativo da errore sincronizzazione** è zero, il telefono non tenta di risincronizzarsi dopo un tentativo di risincronizzazione non riuscito.

Passaggio 8 (Facoltativo) Impostare il valore del campo **Resync Error Retry Delay** su un numero piccolo, come ad esempio **30**.

```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```

Passaggio 9 Disabilitare il server TFTP e osservare i risultati nell'output syslog.

Profili univoci, espansione macro e HTTP

In una distribuzione in cui ogni telefono deve essere configurato con valori distinti per alcuni parametri, ad esempio User_ID o Display_Name, il provider di servizi può creare un profilo univoco per ciascun dispositivo distribuito e ospitare tali profili su un server di provisioning. Ogni telefono, a sua volta, deve essere configurato per risincronizzarsi al proprio profilo in base a una convenzione di denominazione del profilo predeterminato.

La sintassi dell'URL del profilo può includere le informazioni di identificazione che sono specifiche per ogni telefono, ad esempio l'indirizzo MAC o il numero di serie, utilizzando l'espansione macro delle variabili predefinite. L'espansione macro elimina la necessità di specificare questi valori in più posizioni all'interno di ogni profilo.

Una regola del profilo viene sottoposta all'espansione macro prima che la regola applicata la regola venga applicata al telefono. L'espansione macro controlla un numero di valori, ad esempio:

- $MA espande un indirizzo MAC a 12 cifre dell'unità (utilizzando cifre esadecimali minuscole). Ad esempio, 000e08abcdef.
- $SN espande il numero di serie dell'unità. Ad esempio, 88012BA01234.

Per altri valori si può effettuare l'espansione macro in questo modo, tra cui i parametri per scopi generici, GPP_A tramite GPP_P. Un esempio di questo processo è indicato in Risincronizzazione di TFTP, a pagina

51. L'espansione macro non è limitata al nome del file URL, ma può anche essere applicata a qualsiasi parte del parametro della regola del profilo. Questi parametri sono identificati come $A tramite $P. Per un elenco completo delle variabili disponibili per l'espansione macro, vedere Variabili espansione macro, a pagina 77.

In questo esercizio, su un profilo specifico per un telefono viene eseguito il provisioning su un server TFTP.

Esercizio: provisioning di un profilo del telefono IP specifico su un server TFTP

Procedura

Passaggio 1 Ottenere l'indirizzo MAC del telefono dall'etichetta del prodotto. (L'indirizzo MAC è il numero, utilizzando i numeri e le cifre esadecimali minuscole, ad esempio 000e08aabbcc).

Passaggio 2 Copiare il file di configurazione `basic.txt` (descritto nella sezione Risincronizzazione di TFTP, a pagina 51) su un nuovo file denominato `CP-xxxx-3PCC macaddress.cfg` (sostituendo `xxxx` con il numero del modello e `macaddress` con l'indirizzo MAC del telefono).

Passaggio 3 Spostare il nuovo file nella directory principale virtuale del server TFTP.

Passaggio 4 Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Passaggio 5 Selezionare **Voice** > **Provisioning**.

Passaggio 6 Immettere `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` nel campo **Profile Rule**.

```
<Profile_Rule>
  tftp://192.168.1.200/CP-6841-3PCC$MA.cfg
</Profile_Rule>
```

Passaggio 7 Fare clic su **Submit All Changes**. Ciò causa un immediato riavvio e risincronizzazione.

Quando si verifica la successiva risincronizzazione, il telefono ripristina il nuovo file, espandendo l'espressione macro di $MA nel relativo indirizzo MAC.

HTTP GET Resync

HTTP fornisce un meccanismo di risincronizzazione più affidabile di TFTP poiché HTTP stabilisce una connessione TCP e TFTP utilizza il protocollo UDP che è meno affidabile. Inoltre, i server HTTP offrono migliori funzioni di filtraggio e di registrazione rispetto ai server TFTP.

Sul lato client, il telefono non richiede nessuna impostazione di configurazione speciale sul server per essere in grado di effettuare la risincronizzazione tramite HTTP. La sintassi del parametro Profile_Rule per utilizzare HTTP con il metodo GET è simile alla sintassi utilizzata per TFTP. Se un browser Web standard può ripristinare un profilo dal server HTTP, il telefono deve essere in grado di eseguire anche questa operazione.

Esercizio: risincronizzazione di HTTP GET

Procedura

Passaggio 1 Installare un server HTTP sul PC locale o su un altro host accessibile.

Il server open source Apache può essere scaricato da Internet.

Passaggio 2 Copiare il profilo di configurazione `basic.txt` (descritto in Risincronizzazione di TFTP, a pagina 51) nella directory principale virtuale del server installato.

Passaggio 3 Per verificare la corretta installazione del server e l'accesso del file a `basic.txt`, accedere al profilo con un browser Web.

Passaggio 4 Modificare Profile_Rule del telefono del test per indicare il server HTTP al posto del server TFTP, in modo da scaricare periodicamente il profilo.

Ad esempio, presupponendo che il server HTTP sia all'indirizzo 192.168.1.300, immettere il valore seguente:

```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```

Passaggio 5 Fare clic su **Submit All Changes**. Ciò causa un immediato riavvio e risincronizzazione.

Passaggio 6 Osservare i messaggi syslog inviati dal telefono. Adesso le risincronizzazioni periodiche devono ottenere il profilo dal server HTTP.

Passaggio 7 Nei registri del server HTTP, osservare le modalità in cui le informazioni che identificano il telefono del test vengono visualizzate nel registro degli agenti utente.

Queste informazioni devono includere il produttore, il nome del prodotto, la versione del firmware corrente e il numero di serie.

Il provisioning tramite Cisco XML

Per ciascun telefono, designato come xxxx in questo caso, è possibile eseguire il provisioning tramite le funzioni di Cisco XML.

È possibile inviare un oggetto XML al telefono da un pacchetto di notifica SIP o da un HTTP POST all'interfaccia CGI del telefono: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC estende la funzionalità di Cisco XML per supportare il provisioning tramite un oggetto XML:

```
<CP-xxxx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

Dopo aver ricevuto l'oggetto XML, il telefono scarica il file di provisioning da [profile-rule]. Questa regola utilizza le macro per semplificare lo sviluppo dell'applicazione dei servizi XML.

Risoluzione URL con l'espansione macro

Sottodirectory con più profili sul server forniscono un pratico metodo per la gestione di un numero elevato di dispositivi distribuiti. L'URL del profilo può contenere:

- Un nome del server di provisioning o un indirizzo IP esplicito. Se il profilo identifica il server di provisioning in base al nome, il telefono esegue una ricerca DNS per risolvere il nome.
- Una porta del server non standard specificato nell'URL utilizzando la sintassi standard `:port` dopo il nome del server.

- La sottodirectory all'interno della directory principale virtuale del server in cui è archiviato il profilo, specificato utilizzando una notazione del URL standard e gestita dall'espansione macro.

Ad esempio, il seguente Profile_Rule richiede il file di profilo ($PN.cfg) nella sottodirectory del server `/cisco/config`, dal server TFTP che è in esecuzione sull'host prov.telco.com in attesa di una connessione sulla porta 6900:

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
</Profile_Rule>
```

Un profilo per ciascun telefono può essere identificato nel parametro per scopi generici, con il relativo valore denominato all'interno di una regola del profilo comune tramite l'espansione macro.

Ad esempio, si presuppone che GPP_B sia definito come `Dj6Lmp23Q`.

Profile_Rule contiene il valore:

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

Quando il dispositivo si risincronizza e le macro vengono espanse, il telefono con l'indirizzo MAC di 000e08012345 richiede il profilo con il nome che contiene l'indirizzo MAC del dispositivo al seguente URL:

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

Risincronizzazione HTTPS protetta

Questi meccanismi sono disponibili sul telefono per la risincronizzazione utilizzando un processo di comunicazione protetto:

- Risincronizzazione HTTPS di base
- HTTPS con autenticazione del certificato client
- Contenuto dinamico e di filtraggio del client HTTPS

Risincronizzazione HTTPS di base

HTTPS consente di aggiungere SSL a HTTP per il provisioning remoto in modo che:

- Il telefono è in grado di autenticare il server di provisioning.
- Il server di provisioning è in grado di autenticare il telefono.
- È garantita la riservatezza delle informazioni scambiate tra il telefono e il server di provisioning.

SSL genera ed effettua lo scambio di tasti segreti (simmetrici) per ogni connessione tra il telefono e il server, utilizzando coppie di chiavi pubblica/privata preinstallate nel telefono e nel server di provisioning.

Sul lato client, il telefono non richiede nessuna impostazione di configurazione speciale sul server per essere in grado di effettuare la risincronizzazione tramite HTTPS. La sintassi del parametro Profile_Rule per utilizzare HTTPS con il metodo GET è simile alla sintassi utilizzata per HTTP o TFTP. Se un browser Web standard

può ripristinare un profilo dal server HTTPS, il telefono deve essere in grado di eseguire anche questa operazione.

Oltre a installare un server HTTPS, un certificato del server SSL che Cisco firma, deve essere installato sul server di provisioning. I dispositivi non possono effettuare la risincronizzazione su un server che utilizza HTTPS a meno che il server non fornisca un certificato del server firmato da Cisco. Le istruzioni per la creazione di certificati SSL firmati per i prodotti Voce sono disponibili all'indirizzo https://supportforums.cisco.com/docs/DOC-9852.

Esercizio: risincronizzazione HTTPS di base

Procedura

Passaggio 1 Installare un server HTTPS su un host il cui indirizzo IP è noto al server DNS di rete tramite la traduzione del nome host normale.

Il server open source Apache può essere configurato per fungere da server HTTPS durante l'installazione con il pacchetto mod_ssl open source.

Passaggio 2 Generare una richiesta di firma del certificato del server per il server. Per questa fase, potrebbe essere necessario installare il pacchetto OpenSSL open source o software equivalente. Se si utilizza OpenSSL, il comando per generare il file CSR di base è il seguente:

```
openssl req –new –out provserver.csr
```

Questo comando genera una coppia di chiavi pubblica/privata che viene salvata nel file `privkey.pem`.

Passaggio 3 Inviare il file CSR (provserver.csr) a Cisco per la firma.

Un certificato del server firmato viene restituito (provserver.cert) insieme al certificato principale del client Sipura CA, spacroot.cert.

Per ulteriori informazioni, vedere https://supportforums.cisco.com/docs/DOC-9852

Passaggio 4 Archiviare il certificato del server firmato, il file di coppia di chiavi privata e il certificato principale del client nelle rispettive posizioni appropriate sul server.

Nel caso di un'installazione Apache su Linux, queste posizioni sono in genere le seguenti:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

Passaggio 5 Riavviare il server.

Passaggio 6 Copiare il file di configurazione `basic.txt` (descritto in Risincronizzazione di TFTP, a pagina 51) nella directory principale virtuale del server HTTPS.

Passaggio 7 Verificare il corretto funzionamento del server scaricando `basic.txt` dal server HTTPS utilizzando un browser standard dal PC locale.

Passaggio 8 Controllare il certificato del server fornito dal server.

Il browser probabilmente non riconosce il certificato come valido a meno che il browser non sia stato preconfigurato per accettare Cisco come CA principale. Tuttavia, i telefoni si aspettano che il certificato venga firmato in questo modo.

Modificare Profile_Rule del dispositivo del test per contenere un riferimento al server HTTPS, ad esempio:

```
<Profile_Rule>
https://my.server.com/basic.txt
</Profile_Rule>
```

Questo esempio presuppone che il nome del server HTTPS sia **`my.server.com`**.

Passaggio 9 Fare clic su **Submit All Changes**.

Passaggio 10 Osservare la traccia syslog inviata dal telefono.

Il messaggio di syslog deve indicare che la risincronizzazione ha ottenuto il profilo dal server HTTPS.

Passaggio 11 (Facoltativo) Utilizzare lo strumento analizzatore del protocollo Ethernet sulla subnet del telefono per verificare che i pacchetti vengano crittografati.

In questo esercizio non è stata abilitata la verifica del certificato del client. La connessione tra il telefono e il server è crittografata. Tuttavia, il trasferimento non è sicuro in quanto qualsiasi client può connettersi al server e richiedere il file, provando la conoscenza del nome del file e della posizione della directory. Per la risincronizzazione protetta, il server deve anche autenticare il client, come illustrato nell'esercizio descritto in HTTPS con autenticazione del certificato client, a pagina 59.

HTTPS con autenticazione del certificato client

Nella configurazione predefinita di fabbrica, il server non richiede un certificato client SSL da un client. Il trasferimento del profilo non è protetto perché qualsiasi client può connettersi al server e richiedere il profilo. È possibile modificare la configurazione per abilitare l'autenticazione del client; il server richiede un certificato client per autenticare il telefono prima di accettare una richiesta di connessione.

A causa di questo requisito, non è possibile testare l'operazione di risincronizzazione in modo indipendente utilizzando un browser che non disponga di credenziali corrette. Lo scambio di chiavi SSL entro la connessione HTTPS tra il telefono del test e il server può essere osservato con l'utilità ssldump. La traccia di utilità mostra l'interazione tra client e server.

Esercizio: HTTPS con autenticazione del certificato client

Procedura

Passaggio 1 Abilitare l'autenticazione del certificato client sul server HTTPS.

Passaggio 2 In Apache (v.2) impostare il seguente nel file di configurazione del server:

```
SSLVerifyClient  require
```

Inoltre, assicurarsi che spacroot.cert sia stato archiviato come mostrato nell'esercizio Risincronizzazione HTTPS di base, a pagina 57.

Passaggio 3 Riavviare il server HTTPS e osservare la traccia syslog del telefono.

Adesso ogni risincronizzazione al server esegue l'autenticazione simmetrica, in modo che sia il certificato del server, sia il certificato client siano verificati prima di trasferire il profilo.

Passaggio 4 Utilizzare ssldump per l'acquisizione di una connessione di risincronizzazione tra il telefono e il server HTTPS.

Se la verifica del certificato client è stata abilitata correttamente sul server, la traccia ssldump mostra lo scambio simmetrico di certificati (prima dal server al client, poi dal client al server) prima dei pacchetti crittografati che contengono il profilo.

Con l'autenticazione client abilitata, solo un telefono con indirizzo MAC che corrisponde a un valido certificato client può richiedere il profilo dal server di provisioning. Il server rifiuta una richiesta da un browser normale o da un altro dispositivo non autorizzato.

Contenuto dinamico e di filtraggio del client HTTPS

Se il server HTTPS è configurato per richiedere un certificato client, le informazioni nel certificato identificano la risincronizzazione del telefono e forniscono le informazioni sulla configurazione corrette.

Il server HTTPS rende le informazioni del certificato disponibili per gli script CGI (o i programmi CGI compilati) che vengono richiamati come parte della richiesta di risincronizzazione. Ai fini dell'illustrazione, questo esercizio utilizza il linguaggio di script Perl open source e si presuppone che Apache (v.2) venga utilizzato come server HTTPS.

Procedura

Passaggio 1 Installare Perl sull'host che sta eseguendo il server HTTPS.

Passaggio 2 Generare il seguente script riflettore Perl:

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";

print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'}\n";
print "</GPP_D></flat-profile>";
```

Passaggio 3 Salvare il file con il nome del file `reflect.pl`, con l'autorizzazione eseguibile (chmod 755 su Linux), nella directory degli script CGI del server HTTPS.

Passaggio 4 Verificare l'accessibilità degli script CGI sul server (come in `/cgi-bin/...`).

Passaggio 5 Modificare Profile_Rule sul dispositivo del test per effettuare la risincronizzazione allo script riflettore, come nel seguente esempio:

```
https://prov.server.com/cgi-bin/reflect.pl?
```

Passaggio 6 Fare clic su **Submit All Changes**.

Passaggio 7 Osservare la traccia syslog per garantire una risincronizzazione riuscita.

Passaggio 8 Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Passaggio 9 Selezionare **Voice** > **Provisioning**.

Passaggio 10 Verificare che il parametro GPP_D contenga le informazioni acquisite dallo script.

Queste informazioni contengono il nome del prodotto, l'indirizzo MAC e il numero di serie se il dispositivo del test trasporta a un certificato univoco dal produttore. Le informazioni contengano stringhe di generiche se l'unità è stata prodotta prima della versione 2.0 del firmware.

Uno script simile può determinare le informazioni relative al dispositivo di risincronizzazione e quindi fornire il dispositivo con i valori dei parametri di configurazione appropriati.

Certificati HTTPS

Il telefono fornisce una strategia di provisioning sicura e affidabile che si basa su richieste di HTTPS dal dispositivo al server di provisioning. Sia un certificato del server, sia un certificato client vengono utilizzati per autenticare il telefono per il server e il server per il telefono.

Per utilizzare HTTPS con il telefono, è necessario generare una richiesta di firma del certificato (CSR) e inviarla a Cisco. Il telefono genera un certificato per l'installazione sul server di provisioning. Il telefono accetta il certificato quando cerca di stabilire una connessione HTTPS con il server di provisioning.

Metodologia HTTPS

HTTPS consente di crittografare la comunicazione tra un client e un server, in questo modo protegge i contenuti del messaggio da altri dispositivi di rete. Il metodo di crittografia per il corpo della comunicazione tra un client e il server si basa sulla crittografia a chiave simmetrica. Grazie alla crittografia a chiave simmetrica, un client e un server condividono un'unica chiave segreta su un canale protetto, che viene protetta dalla crittografia a chiave pubblica/privata.

I messaggi crittografati dalla chiave segreta possono essere decrittografati utilizzando la stessa chiave. HTTPS supporta un'ampia gamma di algoritmi di crittografia simmetrica. Il telefono implementa la crittografia simmetrica fino a 256 bit, utilizzando lo standard di crittografia americana (AES), oltre a RC4 a 128 bit.

Inoltre, HTTPS fornisce per l'autenticazione di un server e un client impegnati in una transazione protetta. Questa funzione garantisce che un server di provisioning e di un singolo client non possano falsificati da altri dispositivi in rete. Questa funzionalità è essenziale nel contesto di provisioning di endpoint remoti.

L'autenticazione del client e del server viene eseguita utilizzando la crittografia di chiave pubblica/privata con un certificato che contiene la chiave pubblica. Il testo che viene crittografato con una chiave pubblica può essere decrittografato solo dalla chiave privata corrispondente (o viceversa). Il telefono supporta l'algoritmo di Rivest-Shamir-Adleman (RSA) per la crittografia di chiave pubblica/privata.

Certificato del server SSL

Ciascun server di provisioning protetto invia un certificato del server Secure Sockets Layer (SSL) che Cisco firma direttamente. Il firmware che viene eseguito sul telefono riconosce solo un certificato di Cisco come valido. Quando un client si connette a un server tramite HTTPS, rifiuta qualsiasi certificato del server che non è stato firmato da Cisco.

Questo meccanismo consente di proteggere il provider di servizi dall'accesso non autorizzato al telefono o qualsiasi tentativo di falsificare il server di provisioning. Senza tale protezione,un attacco potrebbe eseguire

di nuovamente il provisioning del telefono, per ottenere le informazioni sulla configurazione o per utilizzare un diverso servizio VoIP. Senza la chiave privata che corrisponde a un certificato del server valido, l'attacco non è in grado di stabilire la comunicazione con il telefono.

Ottenere un certificato del server

Procedura

Passaggio 1 Contattare una persona di supporto Cisco che lavorerà con l'utente sul processo del certificato. Se non si lavora con una persona di supporto specifica, inviare per e-mail la richiesta a ciscosb-certadmin@cisco.com.

Passaggio 2 Generare una chiave privata che verrà utilizzata in una CSR (Richiesta di firma del certificato). La chiave è privata e non è necessario fornire questa chiave al supporto Cisco. Utilizzare open source "openssl" per generare la chiave. Ad esempio:

```
openssl genrsa -out <file.key> 1024
```

Passaggio 3 Generare una CSR che contenga i campi che identificano la propria organizzazione e la posizione. Ad esempio:

```
openssl req -new -key <file.key> -out <file.csr>
```

È necessario disporre delle informazioni seguenti:

- Campo oggetto: immettere il Nome comune (CN) che deve essere avere una sintassi FQDN (nome di dominio completo). Durante l'handshake di autenticazione SSL, il telefono verifica che il certificato sia stato ricevuto dalla macchina in cui viene visualizzato.
- Nome host del server: ad esempio, provserv.domain.com.
- Indirizzo e-mail: immettere un indirizzo e-mail in modo che il supporto clienti possa contattare l'utente se necessario. Questo indirizzo e-mail è visibile nella CSR.

Passaggio 4 Inviare per e-mail la CSR (in formato di file zip) alla persona di supporto Cisco o all'indirizzo ciscosb-certadmin@cisco.com. Il certificato viene firmato da Cisco. Cisco invia il certificato all'utente per l'installazione sul sistema.

Certificato client

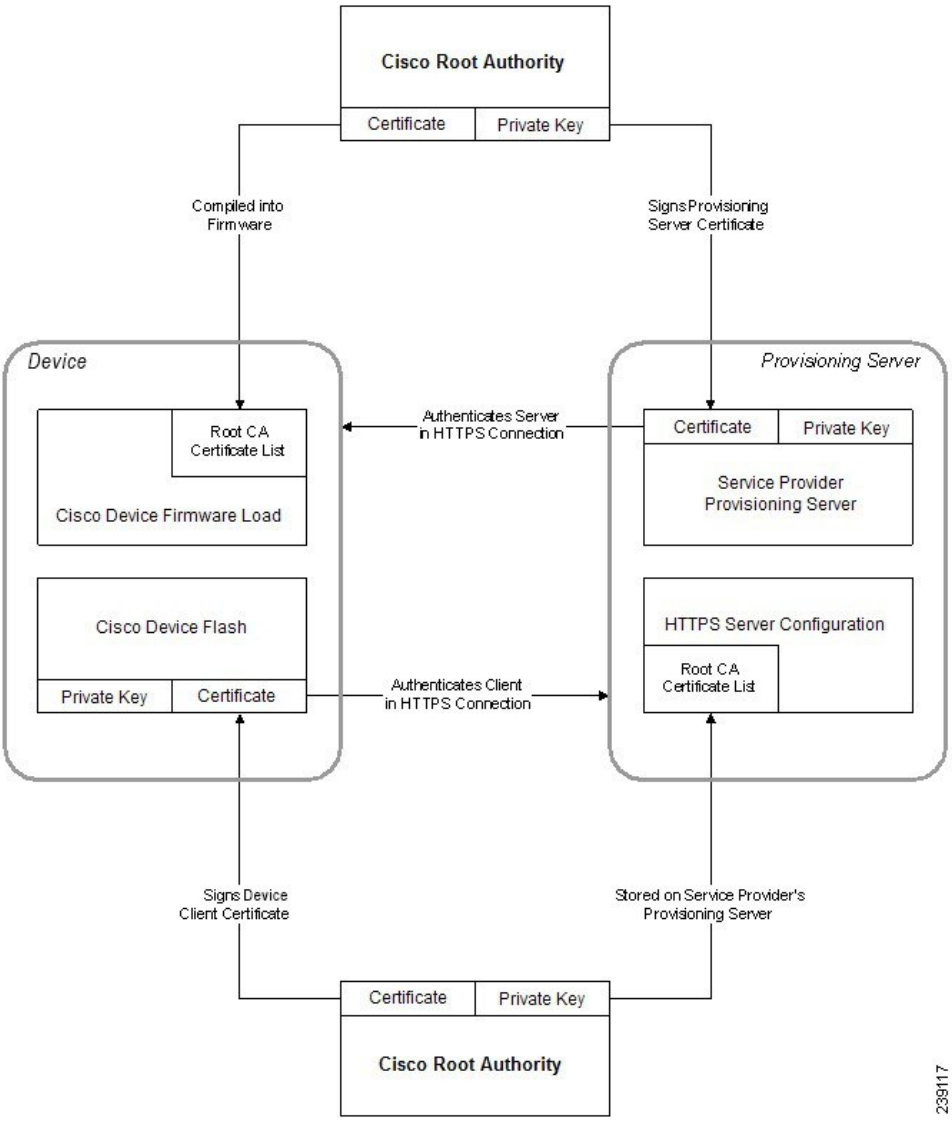
Oltre a un attacco diretto sul telefono, un attacco potrebbe tentare di contattare un server di provisioning mediante un browser Web standard o un altro client HTTPS per ottenere il profilo di configurazione dal server di provisioning. Inoltre, per evitare questo tipo di attacco, ogni telefono contiene un certificato client univoco, firmato da Cisco, che include le informazioni di identificazione di ogni singolo endpoint. Un certificato principale di autorità certificativa che è in grado di autenticare il certificato del client del dispositivo viene assegnato a ogni provider di servizi. Questo percorso di autenticazione consente al server di provisioning di rifiutare le richieste non autorizzate per i profili di configurazione.

Struttura del certificato

La combinazione di un certificato del server e un certificato del client garantisce che la comunicazione sia protetta tra telefono remoto e il rispettivo server di provisioning. La figura riportata di seguito mostra la relazione e la posizione dei certificati, delle coppie di chiavi pubblica/privata e delle autorità principali di firma, tra il client Cisco, il server di provisioning e l'autorità di certificazione.

Nella metà superiore del diagramma mostra l'autorità principale del server di provisioning utilizzata per firmare il singolo certificato del server di provisioning. Il certificato principale corrispondente viene compilato nel firmware, che consente al telefono di autenticare i server di provisioning autorizzati.

Figura 2: Flusso dell'autorità di certificazione



Configurazione di un'autorità certificativa personalizzata

I certificati digitali possono essere utilizzati per autenticare i dispositivi di rete e gli utenti in rete. Possono essere utilizzati per la negoziazione di sessioni IPSec tra i nodi di rete.

Una terza parte utilizza un certificato autorità certificativa per convalidare e autenticare due o più nodi che stanno tentando di comunicare. Ogni nodo dispone di una chiave pubblica e privata. La chiave pubblica crittografa i dati. La chiave privata decrittografa i dati. Poiché i nodi hanno ottenuto i certificati dalla stessa origine, dispongono della garanzia delle rispettive identità.

Il dispositivo può utilizzare i certificati digitali forniti da una terza autorità certificativa (CA) per autenticare le connessioni IPSec.

I telefoni supportano una serie di autorità certificative principali integrate nel firmware:

- Certificato CA per aziende di piccole dimensioni di Cisco
- Certificato CA di CyberTrust
- Certificato CA di VeriSign
- Certificato CA principale di Sipura
- Certificato CA principale di Linksys

Prima di iniziare

Accedere alla pagina Web di amministrazione del telefono. Consultare Accesso alla pagina Web del telefono, a pagina 9.

Procedura

Passaggio 1 Selezionare **Info** > **Status**.

Passaggio 2 Scorrere fino alla voce **Custom CA Status** e vedere i seguenti campi:

- Stato di provisioning di CA personalizzata: indica lo stato di provisioning.
  - Ultimo provisioning completato il gg/mm/aaaa HH:MM:SS oppure
  - Ultimo provisioning non completato il gg/mm/aaaa HH:MM:SS
- Info di CA personalizzata: visualizza le informazioni relative alla CA personalizzata.
  - Installato: visualizza il "Valore CN", ovvero il valore del parametro CN per il campo Oggetto nel primo certificato.
  - Non installato: indica che non è installato alcun certificato CA personalizzato.

Gestione dei profili

In questa sezione viene illustrato la formazione di profili di configurazione in preparazione del download. Per descrivere la funzionalità, TFTP da un PC locale viene utilizzato come metodo di risincronizzazione, sebbene anche HTTP o HTTPS possano essere utilizzati.

Compressione di un profilo Open con Gzip

Un profilo di configurazione in formato XML può assumere dimensioni molto grandi se il profilo specifica tutti i parametri singolarmente. Per ridurre il carico sul server di provisioning, il telefono supporta la

compressione dei file XML, utilizzando il formato di compressione concavo doppio che supporta l'utilità gzip (RFC 1951).

Nota Per consentire al telefono di riconoscere un profilo XML compresso e crittografato, è necessario che la compressione preceda la crittografia.

Per l'integrazione con soluzioni del server di provisioning back-end personalizzate, la libreria di compressione zlib open source può essere utilizzata al posto dell'utilità gzip autonoma per eseguire la compressione del profilo. Tuttavia, il telefono prevede che il file contenga un'intestazione gzip valida.

Procedura

Passaggio 1 Installare gzip sul PC locale.

Passaggio 2 Comprimere la configurazione del profilo `basic.txt` (descritto in Risincronizzazione di TFTP, a pagina 51) richiamando gzip dalla riga di comando:

```
gzip basic.txt
```

Questa operazione genera il file concavo doppio `basic.txt.gz`.

Passaggio 3 Salvare il file `basic.txt.gz` nella directory principale virtuale del server TFTP.

Passaggio 4 Modificare Profile_Rule sul dispositivo del test per risincronizzare il file concavo doppio al posto del file XML originale, come mostrato nell'esempio seguente:

```
tftp://192.168.1.200/basic.txt.gz
```

Passaggio 5 Fare clic su **Submit All Changes**.

Passaggio 6 Osservare la traccia syslog del telefono.

Durante la risincronizzazione, il telefono scarica il nuovo file e questo viene utilizzato per aggiornare i parametri.

Argomenti correlati

Compressione di un profilo Open, a pagina 20

Crittografia di un profilo con OpenSSL

È possibile crittografare un profilo compresso o decompresso (tuttavia, un file deve essere compresso prima di essere crittografato). La crittografia è utile quando alla riservatezza delle informazioni del profilo bisogna prestare particolare attenzione, ad esempio quando viene utilizzato TFTP o HTTP per la comunicazione tra il telefono e il server di provisioning.

Il telefono supporta la crittografia a chiave simmetrica tramite l'algoritmo AES a 256 bit. La crittografia può essere eseguita con il pacchetto open source OpenSSL.

Procedura

Passaggio 1 Installare OpenSSL su un PC locale. Ciò potrebbe richiedere che l'applicazione OpenSSL venga ricompilata per abilitare AES.

Passaggio 2 Utilizzando il file di configurazione `basic.txt` (descritto in Risincronizzazione di TFTP, a pagina 51), generare un file crittografato con il seguente comando:

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

È inoltre possibile utilizzare il file compresso `basic.txt.gz` che è stato creato in Compressione di un profilo Open con Gzip, a pagina 64, poiché il profilo XML può essere sia compresso che crittografato.

Passaggio 3 Archiviare il file crittografato `basic.cfg` nella directory principale virtuale del server TFTP.

Passaggio 4 Modificare Profile_Rule sul dispositivo del test per risincronizzare il file crittografato al posto del file XML originale. La chiave di crittografia viene rilevata sul telefono con la seguente opzione URL:

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

Passaggio 5 Fare clic su **Submit All Changes**.

Passaggio 6 Osservare la traccia syslog del telefono.

Durante la risincronizzazione, il telefono scarica il nuovo file e questo viene utilizzato per aggiornare i parametri.

Argomenti correlati

Crittografia AES-256-CBC, a pagina 21

Creazione di profili partizionati

Un telefono scarica più profili distinti durante ogni risincronizzazione. In questo modo si consente la gestione di diversi tipi di informazioni di profilo su server separati e la manutenzione dei valori del parametro di configurazione comune che sono separati dai valori specifici dell'account.

Procedura

Passaggio 1 Creare un nuovo profilo XML, `basic2.txt`, che consenta di specificare un valore per un parametro che lo renda diverso dagli esercizi precedenti. Ad esempio, per il profilo `basic.txt`, aggiungere il seguente:

```
<GPP_B>ABCD</GPP_B>
```

Passaggio 2 Archiviare il profilo `basic2.txt` nella directory principale virtuale del server TFTP.

Passaggio 3 Lasciare la prima regola del profilo dagli esercizi precedenti nella cartella, ma configurare la seconda regola del profilo (Profile_Rule_B) per indicare il nuovo file:

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
```

```
</Profile_Rule_B>
```

Passaggio 4 Fare clic su **Submit All Changes**.

Adesso il telefono risincronizza sia i primi, sia i secondi profili, in questo ordine, ogni volta che deve essere eseguita un'operazione di risincronizzazione.

Passaggio 5 Osservare la traccia syslog per confermare il comportamento previsto.

Impostazione dell'intestazione privacy del telefono

Un'intestazione privacy utente nel messaggio SIP consente di impostare le esigenze di privacy dell'utente dalla rete attendibile.

È possibile impostare il valore dell'intestazione privacy utente per ciascun interno della linea utilizzando un tag XML nel file `config.xml`.

Le opzioni di intestazione privacy sono:

- Disabled (impostazione predefinita)
- none: l'utente richiede che un servizio di privacy non applichi funzioni di privacy al messaggio SIP.
- header: l'utente necessita di un servizio di privacy per nascondere le intestazioni in cui non è possibile eliminare i dati personali.
- session: l'utente richiede che un servizio di privacy fornisca l'anonimato per le sessioni.
- user: l'utente richiede un livello di privacy solo dagli intermediari.
- id: l'utente richiede che il sistema sostituisca un id che non riveli l'indirizzo IP o il nome host

Procedura

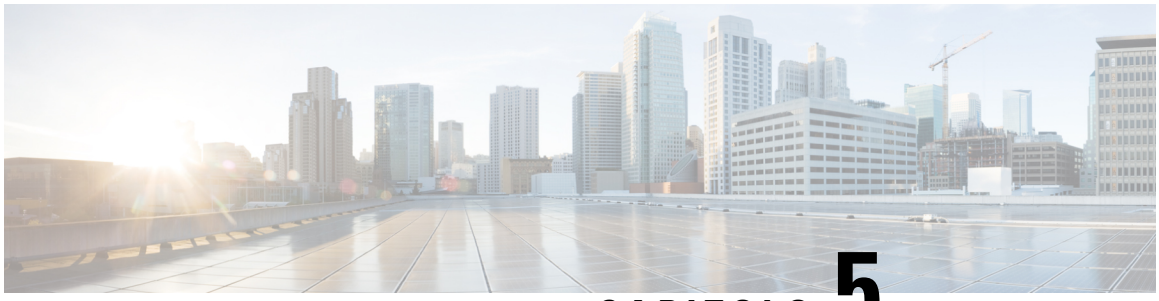
Passaggio 1 Modificare il file `config.xml` in un editor di testo o XML.

Passaggio 2 Inserire il tag **<Privacy_Header_N_ ua="na">*Value*</Privacy_Header_N_>**, dove N è il numero di interno della linea (1-10), e utilizzare uno dei seguenti valori.

- Valore predefinito: **Disabled**
- **nessuno**
- **intestazione**
- **Sessione**
- **utente**
- **id**

Passaggio 3 (Facoltativo) Effettuare il provisioning di eventuali ulteriori interni della linea utilizzando lo stesso tag con il numero di interno della linea richiesta.

Passaggio 4 Salvare le modifiche nel file `config.xml`.



CAPITOLO 5

Parametri di provisioning

Panoramica dei parametri di provisioning

Questo capitolo descrive i parametri di provisioning che possono essere utilizzati negli script dei profili di configurazione.

Parametri di configurazione profili

La seguente tabella definisce la funzione e l'utilizzo di ogni parametro nella sezione **Configuration Profile Parameters** nella scheda **Provisioning**.

Nome del parametro	Descrizione e valore predefinito
Abilita provisioning	Consente di controllare tutte le azioni di risincronizzazione indipendentemente da azioni di aggiornamento del firmware. Impostare su **Yes** per abilitare il provisioning remoto. Il valore predefinito è Sì.
Risincronizza dopo reimpostazione	Attiva la risincronizzazione dopo ogni riavvio del sistema tranne al riavvio dovuto a parametri aggiornamenti e firmware gli aggiornamenti. Il valore predefinito è Sì.

Nome del parametro	Descrizione e valore predefinito
Ritardo casuale risincronizzazione	Un ritardo casuale (in secondi) che segue la sequenza di avvio prima di eseguire la reimpostazione. In un gruppo di dispositivi di telefonia IP pianificati per essere accesi simultaneamente, questo parametro consente di estendere i tempi durante cui ciascuna unità invia una richiesta di risincronizzazione al server di provisioning. Questa funzione può essere utile in un'ampia distribuzione residenziale, in caso di guasto all'alimentazione regionale. Il valore per questo campo deve essere un numero intero compreso tra 0 e 65535. Il valore predefinito è 2.
Risincronizza alle (HHmm)	L'ora (HHmm) in cui il dispositivo si risincronizza con il server di provisioning. Il valore per questo campo deve essere un numero a quattro cifre compreso tra 0000 e 2400 per indicare l'ora nel formato HHmm. Ad esempio, 0959 indica 09:59. Il valore predefinito è vuoto. Se il valore non è valido, il parametro viene ignorato. Se questo parametro è impostato con un valore valido, il parametro di risincronizzazione periodica viene ignorato.
Risincronizza con ritardo casuale	Impedisce a un sovraccarico del server di provisioning quando un numero elevato di dispositivi si accende contemporaneamente. Per evitare di sovraccaricare le richieste di risincronizzazione al server da più telefoni, il telefono si risincronizza nell'intervallo tra le ore e minuti e le ore e minuti più il ritardo casuale (hhmm, hhmm + random_delay). Ad esempio, se il ritardo casuale = (risincronizzazione ritardo casuale + 30)/60 minuti, il valore di input in secondi viene convertito in minuti, con arrotondamento per eccesso al minuto successivo per calcolare l'intervallo finale random_delay. Il valore valido è compreso tra 0 e 65535. Questa funzione è disabilitata quando questo parametro è impostato su zero. Il valore predefinito è 600 secondi (10 minuti).

Nome del parametro	Descrizione e valore predefinito
Risincronizzazione periodica	L'intervallo di tempo tra le sincronizzazioni periodiche si risincronizza con il server di provisioning. Il timer di risincronizzazione associato è attivo solo dopo la prima sincronizzazione corretta con il server. I formati validi sono i seguenti: • Un numero intero Esempio: un input di **`3000`** indica che la risincronizzazione successiva si verifica tra 3000 secondi. • Più numeri interi Esempio: un input di **`600,1200,300`** indica che la prima risincronizzazione si verifica tra 600 secondi, la seconda si verifica tra 1200 secondi dopo la prima e la terza si verifica tra 300 secondi dopo la seconda. • Un intervallo di tempo Esempio: un input di **`2400 + 30`** indica che la risincronizzazione successiva si verifica tra 2400 e 2430 secondi dopo una risincronizzazione eseguita correttamente. Impostare questo parametro su zero per disabilitare la risincronizzazione periodica. Il valore predefinito è 3600 secondi.

Nome del parametro	Descrizione e valore predefinito
Ritardo nuovo tentativo da errore sincronizzazione	Se un'operazione di risincronizzazione non viene completata perché il dispositivo di telefonia IP non è stato in grado di ripristinare un profilo dal server oppure se il file scaricato è danneggiato o si è verificato un errore interno, il dispositivo tenta nuovamente la risincronizzazione dopo un tempo specificato in secondi. I formati validi sono i seguenti: • Un numero intero Esempio: un input di **300** indica che il successivo tentativo di risincronizzazione si verifica in 300 secondi. • Più numeri interi Esempio: un input di **600,1200,300** indica che il primo tentativo si verifica 600 secondi dopo l'errore, il secondo si verifica 1200 secondi dopo l'errore del primo tentativo e il terzo si verifica 300 secondi dopo l'errore del secondo tentativo. • Un intervallo di tempo Esempio: un input di **2400 + 30** indica che il tentativo successivo si verifica tra 2400 e 2430 secondi dopo un errore di risincronizzazione. Se il ritardo è impostato su 0, il dispositivo non tenta nuovamente la risincronizzazione dopo un tentativo di risincronizzazione non riuscito.

Nome del parametro	Descrizione e valore predefinito
Ritardo risincronizzazione forzata	Massimo ritardo (in secondi) che il telefono attende prima di eseguire una risincronizzazione. Il dispositivo non esegue la risincronizzazione mentre una delle sue linee telefoniche è attiva. Una risincronizzazione può richiedere alcuni secondi. È opportuno attendere fino a quando il dispositivo è in stato inattivo per un periodo prolungato prima di eseguire la risincronizzazione. Ciò consente di effettuare chiamate in successione senza interruzioni. Il dispositivo dispone di un timer che inizia il conteggio alla rovescia quando tutte le linee diventano inattive. Questo parametro è il valore iniziale del contatore. Gli eventi di risincronizzazione vengono ritardati fino a quando il contatore non diminuisce fino a raggiungere zero. Il valore valido è compreso tra 0 e 65535. Il valore predefinito è 14400 secondi.
Risincronizza da SIP	Consente di abilitare una risincronizzazione affinché sia attivata tramite un messaggio di NOTIFICA SIP. Il valore predefinito è Sì.
Risincronizzazione dopo tentativo di aggiornamento	Consente di abilitare o disabilitare l'operazione di risincronizzazione dopo qualsiasi aggiornamento. Se è selezionato Yes, la sincronizzazione viene attivata. Il valore predefinito è Sì.
Attivazione risincronizzazione 1, Attivazione risincronizzazione 2	Condizioni di attivazione di risincronizzazione configurabili. La risincronizzazione viene attivata quando l'equazione logica in questi parametri viene valutata come TRUE. Il valore predefinito è vuoto.
Risincronizzazione non riuscita dopo FNF	Una risincronizzazione viene considerata come non riuscita se il server non riceve un profilo richiesto. Ciò può essere ignorato mediante questo parametro. Quando questo parametro è impostato su **No**, il dispositivo accetta una risposta `file-not-found` (file non trovato) dal server come risincronizzazione riuscita. Il valore predefinito è Sì.

Nome del parametro	Descrizione e valore predefinito
Ruolo profilo Regola profilo B Regola profilo C Regola profilo D	Ogni regola profilo indicante il telefono di un'origine da cui ottenere un profilo (file di configurazione). Durante ogni operazione di risincronizzazione, il telefono applica tutti i profili in sequenza. Impostazione predefinita: **`/$PSN.xml`** Se si applica la crittografia AES-256-CBC ai file di configurazione, specificare la chiave di crittografia con la parola chiave **`--key`** nel seguente modo: **`[--key <encryption key>]`** Se lo si desidera, è possibile racchiudere la chiave di crittografia tra virgolette (").
Opzione DHCP da utilizzare	Opzioni DHCP, delimitate da virgole, utilizzate per recuperare firmware e profili. Il valore predefinito è 66,160,159,150,60,43,125.
Messaggio di richiesta registro	Questo parametro contiene il messaggio inviato al server syslog all'inizio di un tentativo di risincronizzazione. Il valore predefinito è `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Messaggio di operazione registro riuscita	Il messaggio del server syslog inviato dopo un tentativo di risincronizzazione riuscito. Il valore predefinito è `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Messaggio di operazione registro non riuscita	Il messaggio del server syslog inviato dopo un tentativo di risincronizzazione non riuscito. Il valore predefinito è `$PN $MAC -- Resync failed: $ERR`.
Risincronizzazione configurabile dall'utente	Consente a un utente di risincronizzare il telefono dallo schermo del telefono IP. Il valore predefinito è Sì.

Parametri di aggiornamento firmware

La seguente tabella definisce la funzione e l'utilizzo di ogni parametro nella sezione **Firmware Upgrade** nella scheda **Provisioning**.

Nome del parametro	Descrizione e valore predefinito
Descrizione	Consente tutte le azioni di risincronizzazione indipendentemente da azioni di aggiornamento del firmware. Il valore predefinito è Sì.
Upgrade Error Retry Delay	Intervallo nuovo tentativo di aggiornamento (in secondi) applicato in caso di errore di aggiornamento. Il dispositivo presenta un firmware timer di errore che consente di attivare dopo un aggiornamento firmware non riuscito tentativo di aggiornamento. Il timer viene avviato con il valore in questo parametro. Il tentativo di aggiornamento firmware successivo si verifica quando questo timer arriva a zero. Il valore predefinito è 3600 secondi.
Regola di aggiornamento	Uno script di aggiornamento firmware che definisce le condizioni di aggiornamento e gli URL firmware associati. Utilizza la stessa sintassi del parametro Profile Rule. Utilizzare il seguente formato per immettere la regola di aggiornamento: **<tftp|http|https>://<indirizzo ip>/image/<nome caricamento>** Ad esempio: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Se non viene specificato alcun protocollo, viene utilizzato il protocollo TFTP. Se non viene specificato alcun nome server, viene utilizzato il nome dell'host che richiede l'URL. Se non viene specificata alcuna porta, viene utilizzata la porta predefinita (69 per TFTP, 80 per HTTP o 443 per HTTPS). Il valore predefinito è vuoto.
Log Upgrade Request Msg	Messaggio del server syslog inviato all'inizio di un tentativo di aggiornamento del firmware. Impostazione predefinita: `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Messaggio del server syslog inviato dopo un tentativo di aggiornamento del firmware riuscito. Il valore predefinito è `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`

Nome del parametro	Descrizione e valore predefinito
Log Upgrade Failure Msg	Messaggio del server syslog inviato dopo un tentativo di aggiornamento del firmware non riuscito. Il valore predefinito è `$PN $MAC -- Upgrade failed: $ERR`
Peer Firmware Sharing	Consente di abilitare o disabilitare la funzionalità di condivisione del firmware. Selezionare **Yes** per abilitare la funzione o **No** per disabilitarla. Impostazione predefinita: Sì
Peer Firmware Sharing Log Server	Indica l'indirizzo IP e la porta a cui viene inviato il messaggio UDP. Ad esempio: 10.98.76.123:514, dove 10.98.76.123 è l'indirizzo IP e 514 è il numero di porta.

Parametri per scopi generici

La seguente tabella definisce la funzione e l'utilizzo di ogni parametro nella sezione **General Purpose Parameters** nella scheda **Provisioning**.

Nome del parametro	Descrizione e valore predefinito
GPP A - GPP P	I parametri per scopi generici GPP_* vengono utilizzati come registri a stringa libera durante la configurazione di telefono per interagire con una specifica soluzione server di provisioning. Possono essere configurati per contenere diversi valori, inclusi i seguenti: • Chiavi di crittografia. • URL. • Informazioni sullo stato del provisioning multifase. • Modelli di richiesta POST. • Mappe alias dei nomi dei parametri. • Valori stringa parziali, eventualmente combinati in valori parametro completi. Il valore predefinito è vuoto.

Variabili espansione macro

Determinate variabili macro vengono riconosciute all'interno dei parametri di provisioning seguenti:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (specifiche condizioni)

All'interno di questi parametri, vengono riconosciuti ed estesi tipi di sintassi quali $NAME o $(NAME).

È possibile specificare sottostringhe variabile macro con la nota $(NAME:p) e $(NAME:p:q), dove p e q sono numeri interi non negativi (disponibile nelle revisioni 2.0.11 e successive). L'espansione macro risultante è la sottostringa che inizia a differenza di carattere p, con lunghezza q (o in caso contrario fino a fine stringa se non è specificato q). Ad esempio, se GPP_A contiene ABCDEF, quindi $(A:2) si espande a CDEF, e $(A:2:3) si espande a CDE.

Un nome non riconosciuto non è stato tradotto e il modulo $NAME o $(NAME) resta invariato nel valore del parametro dopo l'espansione.

Nome del parametro	Descrizione e valore predefinito
$	La forma $$ si espande in un singolo carattere $.
Da A a P	Sostituito dal contenuto dei parametri per scopi generici GPP_A through GPP_P.
Da SA a SD	Sostituiti dai parametri speciali da GPP_SA a GPP_SD. Questi parametri includono i tasti o le password utilizzati per il provisioning. **Nota** I parametri da $SA a $SD vengono riconosciuti come argomenti per il qualificatore dell'URL di risincronizzazione opzionale "--key".
MA	Indirizzo MAC con cifre esadecimali minuscole come ad esempio 000e08aabbcc.
MAU	Indirizzo MAC con cifre esadecimali maiuscole (000E08AABBCC).
MAC	Indirizzo MAC con cifre esadecimali minuscole e due punti come separatore delle coppie di cifre esadecimali, ad esempio 00:0e:08:aa:bb:cc.
PN	Nome prodotto. Ad esempio, CP-6841-3PCC.

Nome del parametro	Descrizione e valore predefinito
PSN	Numero di serie del prodotto. Ad esempio, 6841-3PCC.
SN	Stringa del numero di serie, ad esempio 88012BA01234.
CCERT	Stato del certificato client SSL: Installato o NOn installato.
IP	Indirizzo IP del telefono nella propria subnet locale. Ad esempio 192.168.1.100.
EXTIP	Indirizzo IP esterno del telefono, come visualizzato su Internet. Ad esempio 66.43.16.52.
SWVER	Stringa della versione del software. Ad esempio, sip68xx.11-0-1MPP.
HWVER	Stringa della versione dell'hardware. Ad esempio, 2.0.1
PRVST	Stato del provisioning (stringa numerica): -1 = richiesta di risincronizzazione esplicita 0 = risincronizzazione all'accensione 1 = risincronizzazione periodica 2 = risincronizzazione non riuscita, nuovo tentativo
UPGST	Stato dell'aggiornamento (stringa numerica): 1 = primo tentativo di aggiornamento 2 =aggiornamento non riuscito, nuovo tentativo
UPGERR	Risultato (ERR) del tentativo di aggiornamento precedente; ad esempio http_get non riuscito.
PRVTMR	Secondi dall'ultimo tentativo di risincronizzazione.
UPGTMR	Secondi dall'ultimo tentativo di aggiornamento.
REGTMR1	Secondi dalla mancata registrazione della Linea 1 con il server SIP.
REGTMR2	Secondi dalla mancata registrazione della Linea 2 con il server SIP.
UPGCOND	Nome macro precedente.
SCHEME	Schema di accesso di file (uno tra TFTP, HTTP o HTTPS), ottenuto dopo l'analisi di risincronizzazione o aggiornamento dell'URL.

Nome del parametro	Descrizione e valore predefinito
SERV	Richiedere il nome dell'host del server di destinazione, come ottenuto dopo l'analisi di risincronizzazione o aggiornamento dell'URL.
SERVIP	Richiedere l'indirizzo IP del server di destinazione, come ottenute dopo l'analisi di risincronizzazione o aggiornamento dell'URL, eventualmente seguendo ricerca DNS.
PORTA	Richiedere porta UDP/TCP di destinazione, come ottenuto dopo l'analisi di risincronizzazione o aggiornamento dell'URL.
PATH	Richiedere percorso file di destinazione, come ottenuto dopo l'analisi di risincronizzazione o aggiornamento dell'URL.
ERR	Risultato del tentativo di risincronizzazione o aggiornamento. Solo utili per la generazione di messaggi syslog di risultato. Il valore viene mantenuto nella variabile UPGERR nel caso di tentativi di aggiornamento.
UIDn	Il contenuto del parametro di configurazione UserID per la linea n.
EMS	Stato di Extension Mobility
MUID	ID utente Extension Mobility
MPWD	Password di Extension Mobility

Codici di errore interni

Il telefono definisce una serie di codici di errore interni (X00 – X 99) per agevolare la configurazione fornendo controllo più preciso del comportamento dell'unità in determinate condizioni di errore.

Nome del parametro	Descrizione e valore predefinito
X00	Errore livello di trasporto (o ICMP) quando si invia una richiesta SIP.
X20	La richiesta SIP entra in timeout quando in attesa di una risposta.
X40	Errore del protocollo SIP generale (ad esempio, codec non accettabile in SDP nei messaggi 200 e ACK o entra in timeout durante l'attesa di ACK).

Nome del parametro	Descrizione e valore predefinito
X60	Numero composto non valido in base al piano di numerazione dato.

APPENDICE A

Profili di configurazione di esempio

Esempio di formato Open XML

```
<flat-profile>
 <!--  System Configuration  -->
<Restricted_Access_Domains ua="na"/>
<Enable_Web_Server ua="na">Yes</Enable_Web_Server>
<Enable_Protocol ua="na">Http</Enable_Protocol>
<!--  available options: Http|Https  -->
<Enable_Direct_Action_Url ua="na">Yes</Enable_Direct_Action_Url>
<Session_Max_Timeout ua="na">3600</Session_Max_Timeout>
<Session_Idle_Timeout ua="na">3600</Session_Idle_Timeout>
<Web_Server_Port ua="na">80</Web_Server_Port>
<Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access>
 <!--  <Admin_Password ua="na"/>  -->
 <!--  <User_Password ua="rw"/>  -->
<Phone-UI-readonly ua="na">No</Phone-UI-readonly>
<Phone-UI-User-Mode ua="na">No</Phone-UI-User-Mode>
<User_Password_Prompt ua="na">Yes</User_Password_Prompt>
<Block_Nonproxy_SIP ua="na">No</Block_Nonproxy_SIP>
 <!--  Power Settings  -->
<PoE_Power_Required ua="na">Normal</PoE_Power_Required>
<!--  available options: Normal|Maximum  -->
 <!--  Network Settings  -->
<IP_Mode ua="rw">Dual Mode</IP_Mode>
<!--  available options: IPv4 Only|IPv6 Only|Dual Mode  -->
 <!--  IPv4 Settings  -->
<Connection_Type ua="rw">DHCP</Connection_Type>
<!--  available options: DHCP|Static IP  -->
<Static_IP ua="rw"/>
<NetMask ua="rw"/>
<Gateway ua="rw"/>
<Primary_DNS ua="rw"/>
<Secondary_DNS ua="rw"/>
 <!--  IPv6 Settings  -->
<IPv6_Connection_Type ua="rw">DHCP</IPv6_Connection_Type>
<!--  available options: DHCP|Static IP  -->
<IPv6_Static_IP ua="rw"/>
<Prefix_Length ua="rw">1</Prefix_Length>
<IPv6_Gateway ua="rw"/>
<IPv6_Primary_DNS ua="rw"/>
<IPv6_Secondary_DNS ua="rw"/>
<Broadcast_Echo ua="rw">Disabled</Broadcast_Echo>
```

```
<!--  available options: Disabled|Enabled  -->
<Auto_Config ua="rw">Enabled</Auto_Config>
<!--  available options: Disabled|Enabled  -->
 <!--  802.1X Authentication  -->
<Enable_802.1X_Authentication ua="rw">No</Enable_802.1X_Authentication>
 <!--  Optional Network Configuration  -->
<Host_Name ua="rw"/>
<Domain ua="rw"/>
<DNS_Server_Order ua="na">Manual,DHCP</DNS_Server_Order>
<!--  available options: Manual|Manual,DHCP|DHCP,Manual  -->
<DNS_Query_Mode ua="na">Parallel</DNS_Query_Mode>
<!--  available options: Parallel|Sequential  -->
<DNS_Caching_Enable ua="na">Yes</DNS_Caching_Enable>
<Switch_Port_Config ua="na">AUTO</Switch_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_Port_Config ua="na">AUTO</PC_Port_Config>
<!--
 available options: AUTO|10 HALF|10 FULL|100 HALF|100 FULL|1000 FULL
-->
<PC_PORT_Enable ua="na">Yes</PC_PORT_Enable>
<Enable_PC_Port_Mirror ua="na">No</Enable_PC_Port_Mirror>
<Syslog_Server ua="na"/>
<Syslog_Identifier ua="na">None</Syslog_Identifier>
<!--  available options: None|$MA|$MAU|$MAC|$SN  -->
<Debug_Level ua="na">NOTICE</Debug_Level>
<!--
 available options: EMERGENCY|ALERT|CRITICAL|ERROR|WARNING|NOTICE|INFO|DEBUG
-->
<Primary_NTP_Server ua="rw"/>
<Secondary_NTP_Server ua="rw"/>
<Enable_SSLv3 ua="na">No</Enable_SSLv3>
<Use_Config_TOS ua="na">No</Use_Config_TOS>
 <!--  VLAN Settings  -->
<Enable_VLAN ua="rw">No</Enable_VLAN>
<VLAN_ID ua="rw">1</VLAN_ID>
<PC_Port_VLAN_ID ua="na">1</PC_Port_VLAN_ID>
<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<DHCP_VLAN_Option ua="na"/>
 <!--  Wi-Fi Settings  -->
<Phone-wifi-on ua="rw">Yes</Phone-wifi-on>
<Phone-wifi-type ua="na">WLAN</Phone-wifi-type>
<!--  available options: WLAN|WPS  -->
 <!--  Wi-Fi Profile 1  -->
<Network_Name_1_ ua="rw">wipp</Network_Name_1_>
<Security_Mode_1_ ua="rw">Auto</Security_Mode_1_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_1_ ua="rw">user1</Wi-Fi_User_ID_1_>
 <!--
 <Wi-Fi_Password_1_ ua="rw">**********</Wi-Fi_Password_1_>
-->
 <!--  <WEP_Key_1_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_1_ ua="rw"/>  -->
<Frequency_Band_1_ ua="rw">Auto</Frequency_Band_1_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_1_ ua="rw">1</Wi-Fi_Profile_Order_1_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 2  -->
<Network_Name_2_ ua="rw">internet</Network_Name_2_>
```

```
<Security_Mode_2_ ua="rw">None</Security_Mode_2_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_2_ ua="rw"/>
 <!--  <Wi-Fi_Password_2_ ua="rw"/>  -->
 <!--  <WEP_Key_2_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_2_ ua="rw"/>  -->
<Frequency_Band_2_ ua="rw">Auto</Frequency_Band_2_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_2_ ua="rw">2</Wi-Fi_Profile_Order_2_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 3  -->
<Network_Name_3_ ua="rw"/>
<Security_Mode_3_ ua="rw">None</Security_Mode_3_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_3_ ua="rw"/>
 <!--  <Wi-Fi_Password_3_ ua="rw"/>  -->
 <!--  <WEP_Key_3_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_3_ ua="rw"/>  -->
<Frequency_Band_3_ ua="rw">Auto</Frequency_Band_3_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_3_ ua="rw">3</Wi-Fi_Profile_Order_3_>
<!--  available options: 1|2|3|4  -->
 <!--  Wi-Fi Profile 4  -->
<Network_Name_4_ ua="rw"/>
<Security_Mode_4_ ua="rw">None</Security_Mode_4_>
<!--
 available options: Auto|EAP-FAST|PEAP-GTC|PEAP-MSCHAPV2|PSK|WEP|None
-->
<Wi-Fi_User_ID_4_ ua="rw"/>
 <!--  <Wi-Fi_Password_4_ ua="rw"/>  -->
 <!--  <WEP_Key_4_ ua="rw"/>  -->
 <!--  <PSK_Passphrase_4_ ua="rw"/>  -->
<Frequency_Band_4_ ua="rw">Auto</Frequency_Band_4_>
<!--  available options: Auto|2.4 GHz|5 GHz  -->
<Wi-Fi_Profile_Order_4_ ua="rw">4</Wi-Fi_Profile_Order_4_>
<!--  available options: 1|2|3|4  -->
 <!--  Inventory Settings  -->
<Asset_ID ua="na"/>
 <!--  SIP Parameters  -->
<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<Max_Auth ua="na">2</Max_Auth>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na"/>
<SIP_Accept_Language ua="na"/>
<DTMF_Relay_MIME_Type ua="na">application/dtmf-relay</DTMF_Relay_MIME_Type>
<Hook_Flash_MIME_Type ua="na">application/hook-flash</Hook_Flash_MIME_Type>
<Remove_Last_Reg ua="na">No</Remove_Last_Reg>
<Use_Compact_Header ua="na">No</Use_Compact_Header>
<Escape_Display_Name ua="na">No</Escape_Display_Name>
<Talk_Package ua="na">No</Talk_Package>
<Hold_Package ua="na">No</Hold_Package>
<Conference_Package ua="na">No</Conference_Package>
<RFC_2543_Call_Hold ua="na">Yes</RFC_2543_Call_Hold>
<Random_REG_CID_on_Reboot ua="na">No</Random_REG_CID_on_Reboot>
<SIP_TCP_Port_Min ua="na">5060</SIP_TCP_Port_Min>
<SIP_TCP_Port_Max ua="na">5080</SIP_TCP_Port_Max>
<Caller_ID_Header ua="na">PAID-RPID-FROM</Caller_ID_Header>
<!--
```

Profili di configurazione di esempio

```
 available options: PAID-RPID-FROM|PAID-FROM|RPID-PAID-FROM|RPID-FROM|FROM
-->
<Hold_Target_Before_Refer ua="na">No</Hold_Target_Before_Refer>
<Dialog_SDP_Enable ua="na">No</Dialog_SDP_Enable>
<Keep_Referee_When_Refer_Failed ua="na">No</Keep_Referee_When_Refer_Failed>
<Display_Diversion_Info ua="na">No</Display_Diversion_Info>
<Display_Anonymous_From_Header ua="na">No</Display_Anonymous_From_Header>
<Sip_Accept_Encoding ua="na">none</Sip_Accept_Encoding>
<!--  available options: none|gzip  -->
<SIP_IP_Preference ua="na">IPv4</SIP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
<Disable_Local_Name_To_Header ua="na">No</Disable_Local_Name_To_Header>
 <!--  SIP Timer Values (sec)  -->
<SIP_T1 ua="na">.5</SIP_T1>
<SIP_T2 ua="na">4</SIP_T2>
<SIP_T4 ua="na">5</SIP_T4>
<SIP_Timer_B ua="na">16</SIP_Timer_B>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
<SIP_Timer_H ua="na">16</SIP_Timer_H>
<SIP_Timer_D ua="na">16</SIP_Timer_D>
<SIP_Timer_J ua="na">16</SIP_Timer_J>
<INVITE_Expires ua="na">240</INVITE_Expires>
<ReINVITE_Expires ua="na">30</ReINVITE_Expires>
<Reg_Min_Expires ua="na">1</Reg_Min_Expires>
<Reg_Max_Expires ua="na">7200</Reg_Max_Expires>
<Reg_Retry_Intvl ua="na">30</Reg_Retry_Intvl>
<Reg_Retry_Long_Intvl ua="na">1200</Reg_Retry_Long_Intvl>
<Reg_Retry_Random_Delay ua="na">0</Reg_Retry_Random_Delay>
<Reg_Retry_Long_Random_Delay ua="na">0</Reg_Retry_Long_Random_Delay>
<Reg_Retry_Intvl_Cap ua="na">0</Reg_Retry_Intvl_Cap>
<Sub_Min_Expires ua="na">10</Sub_Min_Expires>
<Sub_Max_Expires ua="na">7200</Sub_Max_Expires>
<Sub_Retry_Intvl ua="na">10</Sub_Retry_Intvl>
 <!--  Response Status Code Handling  -->
<Try_Backup_RSC ua="na"/>
<Retry_Reg_RSC ua="na"/>
 <!--  RTP Parameters  -->
<RTP_Port_Min ua="na">16384</RTP_Port_Min>
<RTP_Port_Max ua="na">16482</RTP_Port_Max>
<RTP_Packet_Size ua="na">0.030</RTP_Packet_Size>
<Max_RTP_ICMP_Err ua="na">0</Max_RTP_ICMP_Err>
<RTCP_Tx_Interval ua="na">0</RTCP_Tx_Interval>
<SDP_IP_Preference ua="na">IPv4</SDP_IP_Preference>
<!--  available options: IPv4|IPv6  -->
 <!--  SDP Payload Types  -->
<G711u_Codec_Name ua="na">PCMU</G711u_Codec_Name>
<G711a_Codec_Name ua="na">PCMA</G711a_Codec_Name>
<G729a_Codec_Name ua="na">G729a</G729a_Codec_Name>
<G729b_Codec_Name ua="na">G729ab</G729b_Codec_Name>
<G722_Codec_Name ua="na">G722</G722_Codec_Name>
<G722.2_Codec_Name ua="na">AMR-WB</G722.2_Codec_Name>
<iLBC_Codec_Name ua="na">iLBC</iLBC_Codec_Name>
<OPUS_Codec_Name ua="na">OPUS</OPUS_Codec_Name>
<AVT_Codec_Name ua="na">telephone-event</AVT_Codec_Name>
<G722.2_Dynamic_Payload ua="na">96</G722.2_Dynamic_Payload>
<G722.2_OA_Dynamic_Payload ua="na">103</G722.2_OA_Dynamic_Payload>
<iLBC_Dynamic_Payload ua="na">97</iLBC_Dynamic_Payload>
<iLBC_30ms_Dynamic_Payload ua="na">105</iLBC_30ms_Dynamic_Payload>
<OPUS_Dynamic_Payload ua="na">99</OPUS_Dynamic_Payload>
<AVT_Dynamic_Payload ua="na">101</AVT_Dynamic_Payload>
<AVT_16kHz_Dynamic_Payload ua="na">107</AVT_16kHz_Dynamic_Payload>
<AVT_48kHz_Dynamic_Payload ua="na">108</AVT_48kHz_Dynamic_Payload>
<INFOREQ_Dynamic_Payload ua="na"/>
 <!--  NAT Support Parameters  -->
```

```
<Handle_VIA_received ua="na">No</Handle_VIA_received>
<Handle_VIA_rport ua="na">No</Handle_VIA_rport>
<Insert_VIA_received ua="na">No</Insert_VIA_received>
<Insert_VIA_rport ua="na">No</Insert_VIA_rport>
<Substitute_VIA_Addr ua="na">No</Substitute_VIA_Addr>
<Send_Resp_To_Src_Port ua="na">No</Send_Resp_To_Src_Port>
<STUN_Enable ua="na">No</STUN_Enable>
<STUN_Test_Enable ua="na">No</STUN_Test_Enable>
<STUN_Server ua="na"/>
<EXT_IP ua="na"/>
<EXT_RTP_Port_Min ua="na">0</EXT_RTP_Port_Min>
<NAT_Keep_Alive_Intvl ua="na">15</NAT_Keep_Alive_Intvl>
<Redirect_Keep_Alive ua="na">No</Redirect_Keep_Alive>
 <!--  Configuration Profile  -->
<Provision_Enable ua="na">Yes</Provision_Enable>
<Resync_On_Reset ua="na">Yes</Resync_On_Reset>
<Resync_Random_Delay ua="na">2</Resync_Random_Delay>
<Resync_At__HHmm_ ua="na"/>
<Resync_At_Random_Delay ua="na">30</Resync_At_Random_Delay>
<Resync_Periodic ua="na">60</Resync_Periodic>
<Resync_Error_Retry_Delay ua="na">360</Resync_Error_Retry_Delay>
<Forced_Resync_Delay ua="na">1440</Forced_Resync_Delay>
<Resync_From_SIP ua="na">Yes</Resync_From_SIP>
<Resync_After_Upgrade_Attempt ua="na">Yes</Resync_After_Upgrade_Attempt>
<Resync_Trigger_1 ua="na"/>
<Resync_Trigger_2 ua="na"/>
<User_Configurable_Resync ua="na">Yes</User_Configurable_Resync>
<Resync_Fails_On_FNF ua="na">Yes</Resync_Fails_On_FNF>
<Profile_Authentication_Type ua="na">Basic Http Authentication</Profile_Authentication_Type>
<!--
 available options: Disabled|Basic Http Authentication|XSI Authentication
-->
<Profile_Rule ua="na">/$PSN-a.xml</Profile_Rule>
<Profile_Rule_B ua="na">/$PSN-b.xml</Profile_Rule_B>
<Profile_Rule_C ua="na"/>
<Profile_Rule_D ua="na"/>
<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>
<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>
<Log_Request_Msg ua="na">
$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Request_Msg>
<Log_Success_Msg ua="na">
$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH
</Log_Success_Msg>
<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>
 <!--  Upload Configuration Options  -->
<Report_Rule ua="na"/>
<HTTP_Report_Method ua="na">POST</HTTP_Report_Method>
<!--  available options: POST|PUT  -->
<Report_To_Server ua="na">On Request</Report_To_Server>
<!--
 available options: On Request|On Local Change|Periodically
-->
<Periodic_Upload_To_Server ua="na">3600</Periodic_Upload_To_Server>
<Upload_Delay_On_Local_Change ua="na">60</Upload_Delay_On_Local_Change>
 <!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na"/>
<Log_Upgrade_Request_Msg ua="na">
$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH
</Log_Upgrade_Request_Msg>
<Log_Upgrade_Success_Msg ua="na">
$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
```

Profili di configurazione di esempio

```
</Log_Upgrade_Success_Msg>
<Log_Upgrade_Failure_Msg ua="na">$PN $MAC -- Upgrade failed: $ERR</Log_Upgrade_Failure_Msg>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Peer_Firmware_Sharing_Log_Server ua="na"/>
 <!--  CA Settings  -->
<Custom_CA_Rule ua="na"/>
 <!--  HTTP Settings  -->
<HTTP_User_Agent_Name ua="na">$VERSION ($MA)</HTTP_User_Agent_Name>
 <!--  Problem Report Tool  -->
<PRT_Upload_Rule ua="na"/>
<PRT_Upload_Method ua="na">POST</PRT_Upload_Method>
<!--  available options: POST|PUT  -->
<PRT_Max_Timer ua="na"/>
<PRT_Name ua="na"/>
 <!--  General Purpose Parameters  -->
<GPP_A ua="na"/>
<GPP_B ua="na"/>
<GPP_C ua="na"/>
<GPP_D ua="na"/>
<GPP_E ua="na"/>
<GPP_F ua="na"/>
<GPP_G ua="na"/>
<GPP_H ua="na"/>
<GPP_I ua="na"/>
<GPP_J ua="na"/>
<GPP_K ua="na"/>
<GPP_L ua="na"/>
<GPP_M ua="na"/>
<GPP_N ua="na"/>
<GPP_O ua="na"/>
<GPP_P ua="na"/>
 <!--  Call Progress Tones  -->
<Dial_Tone ua="na">350@-19,440@-19;10(*/0/1+2)</Dial_Tone>
<Outside_Dial_Tone ua="na">420@-16;10(*/0/1)</Outside_Dial_Tone>
<Prompt_Tone ua="na">520@-19,620@-19;10(*/0/1+2)</Prompt_Tone>
<Busy_Tone ua="na">480@-19,620@-19;10(.5/.5/1+2)</Busy_Tone>
<Reorder_Tone ua="na">480@-19,620@-19;10(.25/.25/1+2)</Reorder_Tone>
<Off_Hook_Warning_Tone ua="na">480@-10,620@0;10(.125/.125/1+2)</Off_Hook_Warning_Tone>
<Ring_Back_Tone ua="na">440@-19,480@-19;*(2/4/1+2)</Ring_Back_Tone>
<Call_Waiting_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Waiting_Tone>
<Confirm_Tone ua="na">600@-16;1(.25/.25/1)</Confirm_Tone>
<MWI_Dial_Tone ua="na">350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)</MWI_Dial_Tone>
<Cfwd_Dial_Tone ua="na">350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2)</Cfwd_Dial_Tone>
<Holding_Tone ua="na">600@-19;25(.1/.1/1,.1/.1/1,.1/9.5/1)</Holding_Tone>
<Conference_Tone ua="na">350@-19;20(.1/.1/1,.1/9.7/1)</Conference_Tone>
<Secure_Call_Indication_Tone
ua="na">397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2)</Secure_Call_Indication_Tone>
<Page_Tone ua="na">600@-16;.3(.05/0.05/1)</Page_Tone>
<Alert_Tone ua="na">600@-19;.2(.05/0.05/1)</Alert_Tone>
<Mute_Tone ua="na">600@-19;.2(.1/0.1/1)</Mute_Tone>
<Unmute_Tone ua="na">600@-19;.3(.1/0.1/1)</Unmute_Tone>
<System_Beep ua="na">600@-16;.1(.05/0.05/1)</System_Beep>
<Call_Pickup_Tone ua="na">440@-10;30(.3/9.7/1)</Call_Pickup_Tone>
 <!--  Distinctive Ring Patterns  -->
<Cadence_1 ua="na">60(2/4)</Cadence_1>
<Cadence_2 ua="na">60(.3/.2,1/.2,.3/4)</Cadence_2>
<Cadence_3 ua="na">60(.8/.4,.8/4)</Cadence_3>
<Cadence_4 ua="na">60(.4/.2,.3/.2,.8/4)</Cadence_4>
<Cadence_5 ua="na">60(.2/.2,.2/.2,.2/.2,1/4)</Cadence_5>
<Cadence_6 ua="na">60(.2/.4,.2/.4,.2/4)</Cadence_6>
<Cadence_7 ua="na">60(4.5/4)</Cadence_7>
<Cadence_8 ua="na">60(0.25/9.75)</Cadence_8>
<Cadence_9 ua="na">60(.4/.2,.4/2)</Cadence_9>
 <!--  Control Timer Values (sec)  -->
```

Profili di configurazione di esempio

```
<Reorder_Delay ua="na">255</Reorder_Delay>
<Interdigit_Long_Timer ua="na">10</Interdigit_Long_Timer>
<Interdigit_Short_Timer ua="na">3</Interdigit_Short_Timer>
 <!--  Vertical Service Activation Codes  -->
<Call_Return_Code ua="na">*69</Call_Return_Code>
<Blind_Transfer_Code ua="na">*95</Blind_Transfer_Code>
<Cfwd_All_Act_Code ua="na">*72</Cfwd_All_Act_Code>
<Cfwd_All_Deact_Code ua="na">*73</Cfwd_All_Deact_Code>
<Cfwd_Busy_Act_Code ua="na">*90</Cfwd_Busy_Act_Code>
<Cfwd_Busy_Deact_Code ua="na">*91</Cfwd_Busy_Deact_Code>
<Cfwd_No_Ans_Act_Code ua="na">*92</Cfwd_No_Ans_Act_Code>
<Cfwd_No_Ans_Deact_Code ua="na">*93</Cfwd_No_Ans_Deact_Code>
<CW_Act_Code ua="na">*56</CW_Act_Code>
<CW_Deact_Code ua="na">*57</CW_Deact_Code>
<CW_Per_Call_Act_Code ua="na">*71</CW_Per_Call_Act_Code>
<CW_Per_Call_Deact_Code ua="na">*70</CW_Per_Call_Deact_Code>
<Block_CID_Act_Code ua="na">*61</Block_CID_Act_Code>
<Block_CID_Deact_Code ua="na">*62</Block_CID_Deact_Code>
<Block_CID_Per_Call_Act_Code ua="na">*81</Block_CID_Per_Call_Act_Code>
<Block_CID_Per_Call_Deact_Code ua="na">*82</Block_CID_Per_Call_Deact_Code>
<Block_ANC_Act_Code ua="na">*77</Block_ANC_Act_Code>
<Block_ANC_Deact_Code ua="na">*87</Block_ANC_Deact_Code>
<DND_Act_Code ua="na">*78</DND_Act_Code>
<DND_Deact_Code ua="na">*79</DND_Deact_Code>
<Secure_All_Call_Act_Code ua="na">*16</Secure_All_Call_Act_Code>
<Secure_No_Call_Act_Code ua="na">*17</Secure_No_Call_Act_Code>
<Secure_One_Call_Act_Code ua="na">*18</Secure_One_Call_Act_Code>
<Secure_One_Call_Deact_Code ua="na">*19</Secure_One_Call_Deact_Code>
<Paging_Code ua="na">*96</Paging_Code>
<Call_Park_Code ua="na">*68</Call_Park_Code>
<Call_Pickup_Code ua="na">*97</Call_Pickup_Code>
<Call_Unpark_Code ua="na">*88</Call_Unpark_Code>
<Group_Call_Pickup_Code ua="na">*98</Group_Call_Pickup_Code>
<Referral_Services_Codes ua="na"/>
<Feature_Dial_Services_Codes ua="na"/>
 <!--  Vertical Service Announcement Codes  -->
<Service_Annc_Base_Number ua="na"/>
<Service_Annc_Extension_Codes ua="na"/>
 <!--  Outbound Call Codec Selection Codes  -->
<Prefer_G711u_Code ua="na">*017110</Prefer_G711u_Code>
<Force_G711u_Code ua="na">*027110</Force_G711u_Code>
<Prefer_G711a_Code ua="na">*017111</Prefer_G711a_Code>
<Force_G711a_Code ua="na">*027111</Force_G711a_Code>
<Prefer_G722_Code ua="na">*01722</Prefer_G722_Code>
<Force_G722_Code ua="na">*02722</Force_G722_Code>
<Prefer_G722.2_Code ua="na">*01724</Prefer_G722.2_Code>
<Force_G722.2_Code ua="na">*02724</Force_G722.2_Code>
<Prefer_G729a_Code ua="na">*01729</Prefer_G729a_Code>
<Force_G729a_Code ua="na">*02729</Force_G729a_Code>
<Prefer_iLBC_Code ua="na">*01016</Prefer_iLBC_Code>
<Force_iLBC_Code ua="na">*02016</Force_iLBC_Code>
<Prefer_OPUS_Code ua="na">*01056</Prefer_OPUS_Code>
<Force_OPUS_Code ua="na">*02056</Force_OPUS_Code>
 <!--  Time  -->
<Set_Local_Date__mm_dd_yyyy_ ua="na"/>
<Set_Local_Time__HH_mm_ ua="na"/>
<Time_Zone ua="na">GMT-06:00</Time_Zone>
<!--
 available options:
[illegible]

-->
<Time_Offset__HH_mm_ ua="na">-00/08</Time_Offset__HH_mm_>
<Ignore_DHCP_Time_Offset ua="na">Yes</Ignore_DHCP_Time_Offset>
```

Profili di configurazione di esempio

```
<Daylight_Saving_Time_Rule
ua="na">start=3/-1/7/2;end=10/-1/7/2;save=1</Daylight_Saving_Time_Rule>
<Daylight_Saving_Time_Enable ua="na">Yes</Daylight_Saving_Time_Enable>
 <!--  Language  -->
<Dictionary_Server_Script ua="na"/>
<Language_Selection ua="na">English-US</Language_Selection>
<Locale ua="na">en-US</Locale>
<!--
 available options:
en-US|en-CA|en-AU|en-GB|fr-FR|fr-CA|es-ES|it-IT|de-DE|nn-NO|pt-PT|nl-NL|sv-SE|pt-BZ|es-MX|en-NZ|da-DK|ru-RU|pl-PL|tr-TR|cs-CZ|hu-HU|fi-FI|sk-SK|bg-BG|hr-HR|ja-JP|ko-KR|zh-CN|zh-HK

-->
 <!--  General  -->
<Station_Name ua="na">arupiSSomSok</Station_Name>
<Station_Display_Name ua="na">RCDN Time</Station_Display_Name>
<Voice_Mail_Number ua="na"/>
<WideBand_Handset_Enable ua="na">No</WideBand_Handset_Enable>
 <!--  Video Configuration  -->
 <!--  Handsfree  -->
<Bluetooth_Mode ua="na">Phone</Bluetooth_Mode>
<!--  available options: Phone|Handsfree|Both  -->
<Line ua="na">5</Line>
<!--
 available options: 1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|Disabled
-->
<Extension_1_ ua="na">1</Extension_1_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_1_ ua="na">$USER hot</Short_Name_1_>
<Share_Call_Appearance_1_ ua="na">private</Share_Call_Appearance_1_>
<!--  available options: private|shared  -->
<Extended_Function_1_ ua="na"/>
<Extension_2_ ua="na">2</Extension_2_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_2_ ua="na">$USER</Short_Name_2_>
<Share_Call_Appearance_2_ ua="na">private</Share_Call_Appearance_2_>
<!--  available options: private|shared  -->
<Extended_Function_2_ ua="na"/>
<Extension_3_ ua="na">3</Extension_3_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_3_ ua="na">$USER</Short_Name_3_>
<Share_Call_Appearance_3_ ua="na">private</Share_Call_Appearance_3_>
<!--  available options: private|shared  -->
<Extended_Function_3_ ua="na"/>
<Extension_4_ ua="na">4</Extension_4_>
<!--  available options: 1|2|3|4|Disabled  -->
<Short_Name_4_ ua="na">$USER</Short_Name_4_>
<Share_Call_Appearance_4_ ua="na">private</Share_Call_Appearance_4_>
<!--  available options: private|shared  -->
<Extended_Function_4_ ua="na"/>
 <!--  Miscellaneous Line Key Settings  -->
<Line_ID_Mapping ua="na">Vertical First</Line_ID_Mapping>
<!--  available options: Horizontal First|Vertical First  -->
<SCA_Barge-In-Enable ua="na">No</SCA_Barge-In-Enable>
<SCA_Sticky_Auto_Line_Seize ua="na">No</SCA_Sticky_Auto_Line_Seize>
<Call_Appearances_Per_Line ua="na">2</Call_Appearances_Per_Line>
<!--  available options: 2|3|4|5|6|7|8|9|10  -->
 <!--  Supplementary Services  -->
<Conference_Serv ua="na">Yes</Conference_Serv>
<Attn_Transfer_Serv ua="na">Yes</Attn_Transfer_Serv>
<Blind_Transfer_Serv ua="na">Yes</Blind_Transfer_Serv>
<DND_Serv ua="na">Yes</DND_Serv>
<Block_ANC_Serv ua="na">Yes</Block_ANC_Serv>
<Block_CID_Serv ua="na">Yes</Block_CID_Serv>
<Secure_Call_Serv ua="na">Yes</Secure_Call_Serv>
```

```
<Cfwd_All_Serv ua="na">Yes</Cfwd_All_Serv>
<Cfwd_Busy_Serv ua="na">Yes</Cfwd_Busy_Serv>
<Cfwd_No_Ans_Serv ua="na">Yes</Cfwd_No_Ans_Serv>
<Paging_Serv ua="na">Yes</Paging_Serv>
<Call_Park_Serv ua="na">Yes</Call_Park_Serv>
<Call_Pick_Up_Serv ua="na">Yes</Call_Pick_Up_Serv>
<ACD_Login_Serv ua="na">No</ACD_Login_Serv>
<Group_Call_Pick_Up_Serv ua="na">Yes</Group_Call_Pick_Up_Serv>
<Service_Annc_Serv ua="na">No</Service_Annc_Serv>
<Call_Recording_Serv ua="na">No</Call_Recording_Serv>
<Reverse_Phone_Lookup_Serv ua="na">Yes</Reverse_Phone_Lookup_Serv>
 <!--  Ringtone  -->
<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>
<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>
<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>
<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>
<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>
<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>
<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>
<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>
<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>
<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>
<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>
<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>
<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>
 <!--  Extension Mobility  -->
<EM_Enable ua="na">No</EM_Enable>
<EM_User_Domain ua="na"/>
<Session_Timer_m_ ua="na">480</Session_Timer_m_>
<Countdown_Timer_s_ ua="na">10</Countdown_Timer_s_>
<Preferred_Password_Input_Mode ua="na">Alpha-numeric</Preferred_Password_Input_Mode>
<!--  available options: Alphanumeric|Numeric  -->
 <!--  XSI Phone Service  -->
<XSI_Host_Server ua="na"/>
<XSI_Authentication_Type ua="na">Login Credentials</XSI_Authentication_Type>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID ua="na"/>
 <!--  <Login_Password ua="na"/>  -->
<SIP_Auth_ID ua="na"/>
 <!--  <SIP_Password ua="na"/>  -->
<Directory_Enable ua="na">No</Directory_Enable>
<Directory_Name ua="na"/>
<Directory_Type ua="na">Enterprise</Directory_Type>
<!--
 available options: Enterprise|Group|Personal|Enterprise Common|Group Common
-->
<CallLog_Enable ua="na">No</CallLog_Enable>
<CallLog_Associated_Line ua="na">1</CallLog_Associated_Line>
<!--  available options: 1|2|3|4  -->
<Display_Recents_From ua="na">Phone</Display_Recents_From>
<!--  available options: Phone|Server  -->
 <!--  Broadsoft XMPP  -->
<XMPP_Enable ua="na">No</XMPP_Enable>
<XMPP_Server ua="na"/>
<XMPP_Port ua="na">5222</XMPP_Port>
<XMPP_User_ID ua="na"/>
 <!--  <XMPP_Password ua="na"/>  -->
<Login_Invisible ua="na">No</Login_Invisible>
<XMPP_Retry_Interval ua="na">30</XMPP_Retry_Interval>
 <!--  Informacast  -->
<Page_Service_URL ua="na"/>
 <!--  XML Service  -->
```

Profili di configurazione di esempio

```
<XML_Directory_Service_Name ua="na"/>
<XML_Directory_Service_URL ua="na"/>
<XML_Application_Service_Name ua="na"/>
<XML_Application_Service_URL ua="na"/>
<XML_User_Name ua="na"/>
 <!--  <XML_Password ua="na"/>  -->
<CISCO_XML_EXE_Enable ua="na">No</CISCO_XML_EXE_Enable>
<CISCO_XML_EXE_Auth_Mode ua="na">Local Credential</CISCO_XML_EXE_Auth_Mode>
<!--
 available options: Trusted|Local Credential|Remote Credential
-->
 <!--  Multiple Paging Group Parameters  -->
<Group_Paging_Script ua="na">
pggrp=224.168.168.168:34560;name=All;num=800;listen=yes;
</Group_Paging_Script>
 <!--  LDAP  -->
<LDAP_Dir_Enable ua="na">No</LDAP_Dir_Enable>
<LDAP_Corp_Dir_Name ua="na"/>
<LDAP_Server ua="na"/>
<LDAP_Search_Base ua="na"/>
<LDAP_Client_DN ua="na"/>
<LDAP_Username ua="na"/>
 <!--  <LDAP_Password ua="na"/>  -->
<LDAP_Auth_Method ua="na">None</LDAP_Auth_Method>
<!--  available options: None|Simple|DIGEST-MD5  -->
<LDAP_Last_Name_Filter ua="na"/>
<LDAP_First_Name_Filter ua="na"/>
<LDAP_Search_Item_3 ua="na"/>
<LDAP_Item_3_Filter ua="na"/>
<LDAP_Search_Item_4 ua="na"/>
<LDAP_Item_4_Filter ua="na"/>
<LDAP_Display_Attrs ua="na"/>
<LDAP_Number_Mapping ua="na"/>
 <!--  Programmable Softkeys  -->
<Programmable_Softkey_Enable ua="na">No</Programmable_Softkey_Enable>
<Idle_Key_List ua="na">
em_login;acd_login;acd_logout;astate;avail;unavail;redial;recents;cfwd;dnd;lcr;pickup;gpickup;unpark;em_logout;guestin;guestout;
</Idle_Key_List>
<Missed_Call_Key_List ua="na">lcr|1;miss|4;</Missed_Call_Key_List>
<Off_Hook_Key_List ua="na">
option;redial;cancel;dir;cfwd;dnd;lcr;unpark;pickup;gpickup;
</Off_Hook_Key_List>
<Dialing_Input_Key_List
ua="na">option|1;call|2;delchar|3;cancel|4;left|5;right|6;</Dialing_Input_Key_List>
<Progressing_Key_List ua="na">endcall|2;</Progressing_Key_List>
<Connected_Key_List ua="na">
hold|1;endcall|2;conf|3;xfer|4;bxfer;confLx;xferLx;park;phold;crdstart;crdpause;crdresume;crdstop;dnd;
</Connected_Key_List>
<Start-Xfer_Key_List ua="na">hold|1;endcall|2;xfer|3;dnd;</Start-Xfer_Key_List>
<Start-Conf_Key_List ua="na">hold|1;endcall|2;conf|3;dnd;</Start-Conf_Key_List>
<Conferencing_Key_List ua="na">
hold|1;endcall|2;join|4;phold;crdstart|5;crdpause|5;crdresume|5;crdstop|6;dnd;
</Conferencing_Key_List>
<Releasing_Key_List ua="na">endcall|2;</Releasing_Key_List>
<Hold_Key_List ua="na">resume|1;endcall|2;newcall|3;redial;dir;cfwd;dnd;</Hold_Key_List>
<Ringing_Key_List ua="na">answer|1;ignore|2;</Ringing_Key_List>
<Shared_Active_Key_List
ua="na">newcall|1;barge|2;bargesilent|3;cfwd|4;dnd|5;</Shared_Active_Key_List>
<Shared_Held_Key_List ua="na">resume|1;barge|2;cfwd|3;dnd|4;</Shared_Held_Key_List>
<PSK_1 ua="na"/>
<PSK_2 ua="na"/>
<PSK_3 ua="na"/>
<PSK_4 ua="na"/>
<PSK_5 ua="na"/>
```

```
<PSK_6 ua="na"/>
<PSK_7 ua="na"/>
<PSK_8 ua="na"/>
<PSK_9 ua="na"/>
<PSK_10 ua="na"/>
<PSK_11 ua="na"/>
<PSK_12 ua="na"/>
<PSK_13 ua="na"/>
<PSK_14 ua="na"/>
<PSK_15 ua="na"/>
<PSK_16 ua="na"/>
 <!--  General  -->
<Line_Enable_1_ ua="na">Yes</Line_Enable_1_>
 <!--  Share Line Appearance  -->
<Share_Ext_1_ ua="na">No</Share_Ext_1_>
<Shared_User_ID_1_ ua="na"/>
<Subscription_Expires_1_ ua="na">3600</Subscription_Expires_1_>
<Restrict_MWI_1_ ua="na">No</Restrict_MWI_1_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_1_ ua="na">No</NAT_Mapping_Enable_1_>
<NAT_Keep_Alive_Enable_1_ ua="na">No</NAT_Keep_Alive_Enable_1_>
<NAT_Keep_Alive_Msg_1_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_1_>
<NAT_Keep_Alive_Dest_1_ ua="na">$PROXY</NAT_Keep_Alive_Dest_1_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_1_ ua="na">0x68</SIP_TOS_DiffServ_Value_1_>
<RTP_TOS_DiffServ_Value_1_ ua="na">0xb8</RTP_TOS_DiffServ_Value_1_>
 <!--  SIP Settings  -->
<SIP_Transport_1_ ua="na">UDP</SIP_Transport_1_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_1_ ua="na">5060</SIP_Port_1_>
<SIP_100REL_Enable_1_ ua="na">No</SIP_100REL_Enable_1_>
<EXT_SIP_Port_1_ ua="na">0</EXT_SIP_Port_1_>
<Auth_Resync-Reboot_1_ ua="na">Yes</Auth_Resync-Reboot_1_>
<SIP_Proxy-Require_1_ ua="na"/>
<SIP_Remote-Party-ID_1_ ua="na">No</SIP_Remote-Party-ID_1_>
<Referor_Bye_Delay_1_ ua="na">4</Referor_Bye_Delay_1_>
<Refer-To_Target_Contact_1_ ua="na">No</Refer-To_Target_Contact_1_>
<Referee_Bye_Delay_1_ ua="na">0</Referee_Bye_Delay_1_>
<Refer_Target_Bye_Delay_1_ ua="na">0</Refer_Target_Bye_Delay_1_>
<Sticky_183_1_ ua="na">No</Sticky_183_1_>
<Auth_INVITE_1_ ua="na">No</Auth_INVITE_1_>
<Ntfy_Refer_On_1xx-To-Inv_1_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_1_>
<Set_G729_annexb_1_ ua="na">yes</Set_G729_annexb_1_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_1_ ua="na"/>
<VQ_Report_Interval_1_ ua="na">0</VQ_Report_Interval_1_>
<User_Equal_Phone_1_ ua="na">No</User_Equal_Phone_1_>
<Call_Recording_Protocol_1_ ua="na">SIPREC</Call_Recording_Protocol_1_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_1_ ua="na">Disabled</Privacy_Header_1_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_1_ ua="na">No</P-Early-Media_Support_1_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_1_ ua="na">No</Blind_Attn-Xfer_Enable_1_>
<Message_Waiting_1_ ua="na">No</Message_Waiting_1_>
<Auth_Page_1_ ua="na">No</Auth_Page_1_>
<Default_Ring_1_ ua="rw">1</Default_Ring_1_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
```

```
<Auth_Page_Realm_1_ ua="na"/>
<Conference_Bridge_URL_1_ ua="na"/>
<Conference_Single_Hardkey_1_ ua="na">No</Conference_Single_Hardkey_1_>
 <!--  <Auth_Page_Password_1_ ua="na"/>  -->
<Mailbox_ID_1_ ua="na"/>
<Voice_Mail_Server_1_ ua="na"/>
<Voice_Mail_Subscribe_Interval_1_ ua="na">86400</Voice_Mail_Subscribe_Interval_1_>
<Auto_Ans_Page_On_Active_Call_1_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_1_>
<Feature_Key_Sync_1_ ua="na">No</Feature_Key_Sync_1_>
<Call_Park_Monitor_Enable_1_ ua="na">No</Call_Park_Monitor_Enable_1_>
<Enable_Broadsoft_Hoteling_1_ ua="na">No</Enable_Broadsoft_Hoteling_1_>
<Hoteling_Subscription_Expires_1_ ua="na">3600</Hoteling_Subscription_Expires_1_>
<Secure_Call_Option_1_ ua="na">Optional</Secure_Call_Option_1_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_1_ ua="na">No</Broadsoft_ACD_1_>
<Call_Information_Enable_1_ ua="na">No</Call_Information_Enable_1_>
<Disposition_Code_Enable_1_ ua="na">No</Disposition_Code_Enable_1_>
<Trace_Enable_1_ ua="na">No</Trace_Enable_1_>
<Emergency_Escalation_Enable_1_ ua="na">No</Emergency_Escalation_Enable_1_>
<Queue_Status_Notification_Enable_1_ ua="na">No</Queue_Status_Notification_Enable_1_>
 <!--  Proxy and Registration  -->
<Proxy_1_ ua="na">as1bsoft.sipurash.com</Proxy_1_>
<Outbound_Proxy_1_ ua="na"/>
<Alternate_Proxy_1_ ua="na"/>
<Alternate_Outbound_Proxy_1_ ua="na"/>
<Use_OB_Proxy_In_Dialog_1_ ua="na">Yes</Use_OB_Proxy_In_Dialog_1_>
<Register_1_ ua="na">Yes</Register_1_>
<Make_Call_Without_Reg_1_ ua="na">No</Make_Call_Without_Reg_1_>
<Register_Expires_1_ ua="na">3600</Register_Expires_1_>
<Ans_Call_Without_Reg_1_ ua="na">No</Ans_Call_Without_Reg_1_>
<Use_DNS_SRV_1_ ua="na">No</Use_DNS_SRV_1_>
<DNS_SRV_Auto_Prefix_1_ ua="na">Yes</DNS_SRV_Auto_Prefix_1_>
<Proxy_Fallback_Intvl_1_ ua="na">3600</Proxy_Fallback_Intvl_1_>
<Proxy_Redundancy_Method_1_ ua="na">Normal</Proxy_Redundancy_Method_1_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_1_ ua="na">No</Dual_Registration_1_>
<Auto_Register_When_Failover_1_ ua="na">No</Auto_Register_When_Failover_1_>
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
 <!--  Subscriber Information  -->
<Display_Name_1_ ua="na"/>
<User_ID_1_ ua="na">4085263127</User_ID_1_>
 <!--  <Password_1_ ua="na">**************</Password_1_>  -->
<Auth_ID_1_ ua="na">AUN3127</Auth_ID_1_>
<Reversed_Auth_Realm_1_ ua="na"/>
<SIP_URI_1_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_1_ ua="na"/>
<XSI_Authentication_Type_1_ ua="na">Login Credentials</XSI_Authentication_Type_1_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_1_ ua="na"/>
 <!--  <Login_Password_1_ ua="na"/>  -->
<Anywhere_Enable_1_ ua="na">No</Anywhere_Enable_1_>
<Block_CID_Enable_1_ ua="na">No</Block_CID_Enable_1_>
<DND_Enable_1_ ua="na">No</DND_Enable_1_>
<CFWD_Enable_1_ ua="na">No</CFWD_Enable_1_>
 <!--  Audio Configuration  -->
<Preferred_Codec_1_ ua="na">G711u</Preferred_Codec_1_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_1_ ua="na">No</Use_Pref_Codec_Only_1_>
```

```
<Second_Preferred_Codec_1_ ua="na">Unspecified</Second_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_1_ ua="na">Unspecified</Third_Preferred_Codec_1_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_1_ ua="na">Yes</G711u_Enable_1_>
<G711a_Enable_1_ ua="na">Yes</G711a_Enable_1_>
<G729a_Enable_1_ ua="na">Yes</G729a_Enable_1_>
<G722_Enable_1_ ua="na">Yes</G722_Enable_1_>
<G722.2_Enable_1_ ua="na">Yes</G722.2_Enable_1_>
<iLBC_Enable_1_ ua="na">Yes</iLBC_Enable_1_>
<OPUS_Enable_1_ ua="na">Yes</OPUS_Enable_1_>
<Silence_Supp_Enable_1_ ua="na">No</Silence_Supp_Enable_1_>
<DTMF_Tx_Method_1_ ua="na">Auto</DTMF_Tx_Method_1_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_1_ ua="na">Default</Codec_Negotiation_1_>
<!--  available options: Default|List All  -->
<Encryption_Method_1_ ua="na">AES 128</Encryption_Method_1_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_1_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_1_>
<Caller_ID_Map_1_ ua="na"/>
<Enable_URI_Dialing_1_ ua="na">No</Enable_URI_Dialing_1_>
<Emergency_Number_1_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_1_ ua="na"/>
<Primary_Request_URL_1_ ua="na"/>
<Secondary_Request_URL_1_ ua="na"/>
 <!--  General  -->
<Line_Enable_2_ ua="na">Yes</Line_Enable_2_>
 <!--  Share Line Appearance  -->
<Share_Ext_2_ ua="na">No</Share_Ext_2_>
<Shared_User_ID_2_ ua="na"/>
<Subscription_Expires_2_ ua="na">3600</Subscription_Expires_2_>
<Restrict_MWI_2_ ua="na">No</Restrict_MWI_2_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_2_ ua="na">No</NAT_Mapping_Enable_2_>
<NAT_Keep_Alive_Enable_2_ ua="na">No</NAT_Keep_Alive_Enable_2_>
<NAT_Keep_Alive_Msg_2_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_2_>
<NAT_Keep_Alive_Dest_2_ ua="na">$PROXY</NAT_Keep_Alive_Dest_2_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_2_ ua="na">0x68</SIP_TOS_DiffServ_Value_2_>
<RTP_TOS_DiffServ_Value_2_ ua="na">0xb8</RTP_TOS_DiffServ_Value_2_>
 <!--  SIP Settings  -->
<SIP_Transport_2_ ua="na">UDP</SIP_Transport_2_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_2_ ua="na">5061</SIP_Port_2_>
<SIP_100REL_Enable_2_ ua="na">No</SIP_100REL_Enable_2_>
<EXT_SIP_Port_2_ ua="na">0</EXT_SIP_Port_2_>
<Auth_Resync-Reboot_2_ ua="na">Yes</Auth_Resync-Reboot_2_>
<SIP_Proxy-Require_2_ ua="na"/>
<SIP_Remote-Party-ID_2_ ua="na">No</SIP_Remote-Party-ID_2_>
<Referor_Bye_Delay_2_ ua="na">4</Referor_Bye_Delay_2_>
<Refer-To_Target_Contact_2_ ua="na">No</Refer-To_Target_Contact_2_>
<Referee_Bye_Delay_2_ ua="na">0</Referee_Bye_Delay_2_>
<Refer_Target_Bye_Delay_2_ ua="na">0</Refer_Target_Bye_Delay_2_>
```

Profili di configurazione di esempio

```
<Sticky_183_2_ ua="na">No</Sticky_183_2_>
<Auth_INVITE_2_ ua="na">No</Auth_INVITE_2_>
<Ntfy_Refer_On_1xx-To-Inv_2_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_2_>
<Set_G729_annexb_2_ ua="na">yes</Set_G729_annexb_2_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_2_ ua="na"/>
<VQ_Report_Interval_2_ ua="na">0</VQ_Report_Interval_2_>
<User_Equal_Phone_2_ ua="na">No</User_Equal_Phone_2_>
<Call_Recording_Protocol_2_ ua="na">SIPREC</Call_Recording_Protocol_2_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_2_ ua="na">Disabled</Privacy_Header_2_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_2_ ua="na">No</P-Early-Media_Support_2_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_2_ ua="na">No</Blind_Attn-Xfer_Enable_2_>
<Message_Waiting_2_ ua="na">No</Message_Waiting_2_>
<Auth_Page_2_ ua="na">No</Auth_Page_2_>
<Default_Ring_2_ ua="rw">1</Default_Ring_2_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_2_ ua="na"/>
<Conference_Bridge_URL_2_ ua="na"/>
<Conference_Single_Hardkey_2_ ua="na">No</Conference_Single_Hardkey_2_>
 <!--  <Auth_Page_Password_2_ ua="na"/>  -->
<Mailbox_ID_2_ ua="na"/>
<Voice_Mail_Server_2_ ua="na"/>
<Voice_Mail_Subscribe_Interval_2_ ua="na">86400</Voice_Mail_Subscribe_Interval_2_>
<Auto_Ans_Page_On_Active_Call_2_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_2_>
<Feature_Key_Sync_2_ ua="na">No</Feature_Key_Sync_2_>
<Call_Park_Monitor_Enable_2_ ua="na">No</Call_Park_Monitor_Enable_2_>
<Enable_Broadsoft_Hoteling_2_ ua="na">No</Enable_Broadsoft_Hoteling_2_>
<Hoteling_Subscription_Expires_2_ ua="na">3600</Hoteling_Subscription_Expires_2_>
<Secure_Call_Option_2_ ua="na">Optional</Secure_Call_Option_2_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_2_ ua="na">No</Broadsoft_ACD_2_>
<Call_Information_Enable_2_ ua="na">No</Call_Information_Enable_2_>
<Disposition_Code_Enable_2_ ua="na">No</Disposition_Code_Enable_2_>
<Trace_Enable_2_ ua="na">No</Trace_Enable_2_>
<Emergency_Escalation_Enable_2_ ua="na">No</Emergency_Escalation_Enable_2_>
<Queue_Status_Notification_Enable_2_ ua="na">No</Queue_Status_Notification_Enable_2_>
 <!--  Proxy and Registration  -->
<Proxy_2_ ua="na">10.74.51.158</Proxy_2_>
<Outbound_Proxy_2_ ua="na"/>
<Alternate_Proxy_2_ ua="na"/>
<Alternate_Outbound_Proxy_2_ ua="na"/>
<Use_OB_Proxy_In_Dialog_2_ ua="na">Yes</Use_OB_Proxy_In_Dialog_2_>
<Register_2_ ua="na">Yes</Register_2_>
<Make_Call_Without_Reg_2_ ua="na">No</Make_Call_Without_Reg_2_>
<Register_Expires_2_ ua="na">360</Register_Expires_2_>
<Ans_Call_Without_Reg_2_ ua="na">No</Ans_Call_Without_Reg_2_>
<Use_DNS_SRV_2_ ua="na">No</Use_DNS_SRV_2_>
<DNS_SRV_Auto_Prefix_2_ ua="na">Yes</DNS_SRV_Auto_Prefix_2_>
<Proxy_Fallback_Intvl_2_ ua="na">3600</Proxy_Fallback_Intvl_2_>
<Proxy_Redundancy_Method_2_ ua="na">Normal</Proxy_Redundancy_Method_2_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_2_ ua="na">No</Dual_Registration_2_>
<Auto_Register_When_Failover_2_ ua="na">No</Auto_Register_When_Failover_2_>
<TLS_Name_Validate_2_ ua="na">Yes</TLS_Name_Validate_2_>
```

```
 <!--  Subscriber Information  -->
<Display_Name_2_ ua="na"/>
<User_ID_2_ ua="na">158165</User_ID_2_>
 <!--  <Password_2_ ua="na"/>  -->
<Auth_ID_2_ ua="na"/>
<Reversed_Auth_Realm_2_ ua="na"/>
<SIP_URI_2_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_2_ ua="na"/>
<XSI_Authentication_Type_2_ ua="na">Login Credentials</XSI_Authentication_Type_2_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_2_ ua="na"/>
 <!--  <Login_Password_2_ ua="na"/>  -->
<Anywhere_Enable_2_ ua="na">No</Anywhere_Enable_2_>
<Block_CID_Enable_2_ ua="na">No</Block_CID_Enable_2_>
<DND_Enable_2_ ua="na">No</DND_Enable_2_>
<CFWD_Enable_2_ ua="na">No</CFWD_Enable_2_>
 <!--  Audio Configuration  -->
<Preferred_Codec_2_ ua="na">G711u</Preferred_Codec_2_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_2_ ua="na">No</Use_Pref_Codec_Only_2_>
<Second_Preferred_Codec_2_ ua="na">Unspecified</Second_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_2_ ua="na">Unspecified</Third_Preferred_Codec_2_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_2_ ua="na">Yes</G711u_Enable_2_>
<G711a_Enable_2_ ua="na">Yes</G711a_Enable_2_>
<G729a_Enable_2_ ua="na">Yes</G729a_Enable_2_>
<G722_Enable_2_ ua="na">Yes</G722_Enable_2_>
<G722.2_Enable_2_ ua="na">Yes</G722.2_Enable_2_>
<iLBC_Enable_2_ ua="na">Yes</iLBC_Enable_2_>
<OPUS_Enable_2_ ua="na">Yes</OPUS_Enable_2_>
<Silence_Supp_Enable_2_ ua="na">No</Silence_Supp_Enable_2_>
<DTMF_Tx_Method_2_ ua="na">Auto</DTMF_Tx_Method_2_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_2_ ua="na">Default</Codec_Negotiation_2_>
<!--  available options: Default|List All  -->
<Encryption_Method_2_ ua="na">AES 128</Encryption_Method_2_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_2_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_2_>
<Caller_ID_Map_2_ ua="na"/>
<Enable_URI_Dialing_2_ ua="na">No</Enable_URI_Dialing_2_>
<Emergency_Number_2_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_2_ ua="na"/>
<Primary_Request_URL_2_ ua="na"/>
<Secondary_Request_URL_2_ ua="na"/>
 <!--  General  -->
<Line_Enable_3_ ua="na">Yes</Line_Enable_3_>
 <!--  Share Line Appearance  -->
```

Profili di configurazione di esempio

```
<Share_Ext_3_ ua="na">No</Share_Ext_3_>
<Shared_User_ID_3_ ua="na"/>
<Subscription_Expires_3_ ua="na">3600</Subscription_Expires_3_>
<Restrict_MWI_3_ ua="na">No</Restrict_MWI_3_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_3_ ua="na">No</NAT_Mapping_Enable_3_>
<NAT_Keep_Alive_Enable_3_ ua="na">No</NAT_Keep_Alive_Enable_3_>
<NAT_Keep_Alive_Msg_3_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_3_>
<NAT_Keep_Alive_Dest_3_ ua="na">$PROXY</NAT_Keep_Alive_Dest_3_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_3_ ua="na">0x68</SIP_TOS_DiffServ_Value_3_>
<RTP_TOS_DiffServ_Value_3_ ua="na">0xb8</RTP_TOS_DiffServ_Value_3_>
 <!--  SIP Settings  -->
<SIP_Transport_3_ ua="na">UDP</SIP_Transport_3_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_3_ ua="na">5062</SIP_Port_3_>
<SIP_100REL_Enable_3_ ua="na">No</SIP_100REL_Enable_3_>
<EXT_SIP_Port_3_ ua="na">0</EXT_SIP_Port_3_>
<Auth_Resync-Reboot_3_ ua="na">Yes</Auth_Resync-Reboot_3_>
<SIP_Proxy-Require_3_ ua="na"/>
<SIP_Remote-Party-ID_3_ ua="na">No</SIP_Remote-Party-ID_3_>
<Referor_Bye_Delay_3_ ua="na">4</Referor_Bye_Delay_3_>
<Refer-To_Target_Contact_3_ ua="na">No</Refer-To_Target_Contact_3_>
<Referee_Bye_Delay_3_ ua="na">0</Referee_Bye_Delay_3_>
<Refer_Target_Bye_Delay_3_ ua="na">0</Refer_Target_Bye_Delay_3_>
<Sticky_183_3_ ua="na">No</Sticky_183_3_>
<Auth_INVITE_3_ ua="na">No</Auth_INVITE_3_>
<Ntfy_Refer_On_1xx-To-Inv_3_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_3_>
<Set_G729_annexb_3_ ua="na">yes</Set_G729_annexb_3_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_3_ ua="na"/>
<VQ_Report_Interval_3_ ua="na">0</VQ_Report_Interval_3_>
<User_Equal_Phone_3_ ua="na">No</User_Equal_Phone_3_>
<Call_Recording_Protocol_3_ ua="na">SIPREC</Call_Recording_Protocol_3_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_3_ ua="na">Disabled</Privacy_Header_3_>
<!--
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_3_ ua="na">No</P-Early-Media_Support_3_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_3_ ua="na">No</Blind_Attn-Xfer_Enable_3_>
<Message_Waiting_3_ ua="na">No</Message_Waiting_3_>
<Auth_Page_3_ ua="na">No</Auth_Page_3_>
<Default_Ring_3_ ua="rw">1</Default_Ring_3_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_3_ ua="na"/>
<Conference_Bridge_URL_3_ ua="na"/>
<Conference_Single_Hardkey_3_ ua="na">No</Conference_Single_Hardkey_3_>
 <!--  <Auth_Page_Password_3_ ua="na"/>  -->
<Mailbox_ID_3_ ua="na"/>
<Voice_Mail_Server_3_ ua="na"/>
<Voice_Mail_Subscribe_Interval_3_ ua="na">86400</Voice_Mail_Subscribe_Interval_3_>
<Auto_Ans_Page_On_Active_Call_3_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_3_>
<Feature_Key_Sync_3_ ua="na">No</Feature_Key_Sync_3_>
<Call_Park_Monitor_Enable_3_ ua="na">No</Call_Park_Monitor_Enable_3_>
<Enable_Broadsoft_Hoteling_3_ ua="na">No</Enable_Broadsoft_Hoteling_3_>
<Hoteling_Subscription_Expires_3_ ua="na">3600</Hoteling_Subscription_Expires_3_>
<Secure_Call_Option_3_ ua="na">Optional</Secure_Call_Option_3_>
<!--  available options: Optional|Required  -->
```

```
 <!--  ACD Settings  -->
<Broadsoft_ACD_3_ ua="na">No</Broadsoft_ACD_3_>
<Call_Information_Enable_3_ ua="na">No</Call_Information_Enable_3_>
<Disposition_Code_Enable_3_ ua="na">No</Disposition_Code_Enable_3_>
<Trace_Enable_3_ ua="na">No</Trace_Enable_3_>
<Emergency_Escalation_Enable_3_ ua="na">No</Emergency_Escalation_Enable_3_>
<Queue_Status_Notification_Enable_3_ ua="na">No</Queue_Status_Notification_Enable_3_>
 <!--  Proxy and Registration  -->
<Proxy_3_ ua="na"/>
<Outbound_Proxy_3_ ua="na"/>
<Alternate_Proxy_3_ ua="na"/>
<Alternate_Outbound_Proxy_3_ ua="na"/>
<Use_OB_Proxy_In_Dialog_3_ ua="na">Yes</Use_OB_Proxy_In_Dialog_3_>
<Register_3_ ua="na">Yes</Register_3_>
<Make_Call_Without_Reg_3_ ua="na">No</Make_Call_Without_Reg_3_>
<Register_Expires_3_ ua="na">3600</Register_Expires_3_>
<Ans_Call_Without_Reg_3_ ua="na">No</Ans_Call_Without_Reg_3_>
<Use_DNS_SRV_3_ ua="na">No</Use_DNS_SRV_3_>
<DNS_SRV_Auto_Prefix_3_ ua="na">Yes</DNS_SRV_Auto_Prefix_3_>
<Proxy_Fallback_Intvl_3_ ua="na">3600</Proxy_Fallback_Intvl_3_>
<Proxy_Redundancy_Method_3_ ua="na">Normal</Proxy_Redundancy_Method_3_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_3_ ua="na">No</Dual_Registration_3_>
<Auto_Register_When_Failover_3_ ua="na">No</Auto_Register_When_Failover_3_>
<TLS_Name_Validate_3_ ua="na">Yes</TLS_Name_Validate_3_>
 <!--  Subscriber Information  -->
<Display_Name_3_ ua="na"/>
<User_ID_3_ ua="na"/>
 <!--  <Password_3_ ua="na"/>  -->
<Auth_ID_3_ ua="na"/>
<Reversed_Auth_Realm_3_ ua="na"/>
<SIP_URI_3_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_3_ ua="na"/>
<XSI_Authentication_Type_3_ ua="na">Login Credentials</XSI_Authentication_Type_3_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_3_ ua="na"/>
 <!--  <Login_Password_3_ ua="na"/>  -->
<Anywhere_Enable_3_ ua="na">No</Anywhere_Enable_3_>
<Block_CID_Enable_3_ ua="na">No</Block_CID_Enable_3_>
<DND_Enable_3_ ua="na">No</DND_Enable_3_>
<CFWD_Enable_3_ ua="na">No</CFWD_Enable_3_>
 <!--  Audio Configuration  -->
<Preferred_Codec_3_ ua="na">G711u</Preferred_Codec_3_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_3_ ua="na">No</Use_Pref_Codec_Only_3_>
<Second_Preferred_Codec_3_ ua="na">Unspecified</Second_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_3_ ua="na">Unspecified</Third_Preferred_Codec_3_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_3_ ua="na">Yes</G711u_Enable_3_>
<G711a_Enable_3_ ua="na">Yes</G711a_Enable_3_>
<G729a_Enable_3_ ua="na">Yes</G729a_Enable_3_>
<G722_Enable_3_ ua="na">Yes</G722_Enable_3_>
<G722.2_Enable_3_ ua="na">Yes</G722.2_Enable_3_>
<iLBC_Enable_3_ ua="na">Yes</iLBC_Enable_3_>
```

Profili di configurazione di esempio

```
<OPUS_Enable_3_ ua="na">Yes</OPUS_Enable_3_>
<Silence_Supp_Enable_3_ ua="na">No</Silence_Supp_Enable_3_>
<DTMF_Tx_Method_3_ ua="na">Auto</DTMF_Tx_Method_3_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_3_ ua="na">Default</Codec_Negotiation_3_>
<!--  available options: Default|List All  -->
<Encryption_Method_3_ ua="na">AES 128</Encryption_Method_3_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_3_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_3_>
<Caller_ID_Map_3_ ua="na"/>
<Enable_URI_Dialing_3_ ua="na">No</Enable_URI_Dialing_3_>
<Emergency_Number_3_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_3_ ua="na"/>
<Primary_Request_URL_3_ ua="na"/>
<Secondary_Request_URL_3_ ua="na"/>
 <!--  General  -->
<Line_Enable_4_ ua="na">Yes</Line_Enable_4_>
 <!--  Share Line Appearance  -->
<Share_Ext_4_ ua="na">No</Share_Ext_4_>
<Shared_User_ID_4_ ua="na"/>
<Subscription_Expires_4_ ua="na">3600</Subscription_Expires_4_>
<Restrict_MWI_4_ ua="na">No</Restrict_MWI_4_>
 <!--  NAT Settings  -->
<NAT_Mapping_Enable_4_ ua="na">No</NAT_Mapping_Enable_4_>
<NAT_Keep_Alive_Enable_4_ ua="na">No</NAT_Keep_Alive_Enable_4_>
<NAT_Keep_Alive_Msg_4_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_4_>
<NAT_Keep_Alive_Dest_4_ ua="na">$PROXY</NAT_Keep_Alive_Dest_4_>
 <!--  Network Settings  -->
<SIP_TOS_DiffServ_Value_4_ ua="na">0x68</SIP_TOS_DiffServ_Value_4_>
<RTP_TOS_DiffServ_Value_4_ ua="na">0xb8</RTP_TOS_DiffServ_Value_4_>
 <!--  SIP Settings  -->
<SIP_Transport_4_ ua="na">UDP</SIP_Transport_4_>
<!--  available options: UDP|TCP|TLS|AUTO  -->
<SIP_Port_4_ ua="na">5063</SIP_Port_4_>
<SIP_100REL_Enable_4_ ua="na">No</SIP_100REL_Enable_4_>
<EXT_SIP_Port_4_ ua="na">0</EXT_SIP_Port_4_>
<Auth_Resync-Reboot_4_ ua="na">Yes</Auth_Resync-Reboot_4_>
<SIP_Proxy-Require_4_ ua="na"/>
<SIP_Remote-Party-ID_4_ ua="na">No</SIP_Remote-Party-ID_4_>
<Referor_Bye_Delay_4_ ua="na">4</Referor_Bye_Delay_4_>
<Refer-To_Target_Contact_4_ ua="na">No</Refer-To_Target_Contact_4_>
<Referee_Bye_Delay_4_ ua="na">0</Referee_Bye_Delay_4_>
<Refer_Target_Bye_Delay_4_ ua="na">0</Refer_Target_Bye_Delay_4_>
<Sticky_183_4_ ua="na">No</Sticky_183_4_>
<Auth_INVITE_4_ ua="na">No</Auth_INVITE_4_>
<Ntfy_Refer_On_1xx-To-Inv_4_ ua="na">Yes</Ntfy_Refer_On_1xx-To-Inv_4_>
<Set_G729_annexb_4_ ua="na">yes</Set_G729_annexb_4_>
<!--
 available options: none|no|yes|follow silence supp setting
-->
<Voice_Quality_Report_Address_4_ ua="na"/>
<VQ_Report_Interval_4_ ua="na">0</VQ_Report_Interval_4_>
<User_Equal_Phone_4_ ua="na">No</User_Equal_Phone_4_>
<Call_Recording_Protocol_4_ ua="na">SIPREC</Call_Recording_Protocol_4_>
<!--  available options: SIPREC|SIPINFO  -->
<Privacy_Header_4_ ua="na">Disabled</Privacy_Header_4_>
<!--
```

```
 available options: Disabled|none|header|session|user|id
-->
<P-Early-Media_Support_4_ ua="na">No</P-Early-Media_Support_4_>
 <!--  Call Feature Settings  -->
<Blind_Attn-Xfer_Enable_4_ ua="na">No</Blind_Attn-Xfer_Enable_4_>
<Message_Waiting_4_ ua="na">No</Message_Waiting_4_>
<Auth_Page_4_ ua="na">No</Auth_Page_4_>
<Default_Ring_4_ ua="rw">1</Default_Ring_4_>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12|13|14
-->
<Auth_Page_Realm_4_ ua="na"/>
<Conference_Bridge_URL_4_ ua="na"/>
<Conference_Single_Hardkey_4_ ua="na">No</Conference_Single_Hardkey_4_>
 <!--  <Auth_Page_Password_4_ ua="na"/>  -->
<Mailbox_ID_4_ ua="na"/>
<Voice_Mail_Server_4_ ua="na"/>
<Voice_Mail_Subscribe_Interval_4_ ua="na">86400</Voice_Mail_Subscribe_Interval_4_>
<Auto_Ans_Page_On_Active_Call_4_ ua="na">Yes</Auto_Ans_Page_On_Active_Call_4_>
<Feature_Key_Sync_4_ ua="na">No</Feature_Key_Sync_4_>
<Call_Park_Monitor_Enable_4_ ua="na">No</Call_Park_Monitor_Enable_4_>
<Enable_Broadsoft_Hoteling_4_ ua="na">No</Enable_Broadsoft_Hoteling_4_>
<Hoteling_Subscription_Expires_4_ ua="na">3600</Hoteling_Subscription_Expires_4_>
<Secure_Call_Option_4_ ua="na">Optional</Secure_Call_Option_4_>
<!--  available options: Optional|Required  -->
 <!--  ACD Settings  -->
<Broadsoft_ACD_4_ ua="na">No</Broadsoft_ACD_4_>
<Call_Information_Enable_4_ ua="na">No</Call_Information_Enable_4_>
<Disposition_Code_Enable_4_ ua="na">No</Disposition_Code_Enable_4_>
<Trace_Enable_4_ ua="na">No</Trace_Enable_4_>
<Emergency_Escalation_Enable_4_ ua="na">No</Emergency_Escalation_Enable_4_>
<Queue_Status_Notification_Enable_4_ ua="na">No</Queue_Status_Notification_Enable_4_>
 <!--  Proxy and Registration  -->
<Proxy_4_ ua="na">as1bsoft.sipurash.com</Proxy_4_>
<Outbound_Proxy_4_ ua="na"/>
<Alternate_Proxy_4_ ua="na"/>
<Alternate_Outbound_Proxy_4_ ua="na"/>
<Use_OB_Proxy_In_Dialog_4_ ua="na">Yes</Use_OB_Proxy_In_Dialog_4_>
<Register_4_ ua="na">Yes</Register_4_>
<Make_Call_Without_Reg_4_ ua="na">No</Make_Call_Without_Reg_4_>
<Register_Expires_4_ ua="na">3600</Register_Expires_4_>
<Ans_Call_Without_Reg_4_ ua="na">No</Ans_Call_Without_Reg_4_>
<Use_DNS_SRV_4_ ua="na">No</Use_DNS_SRV_4_>
<DNS_SRV_Auto_Prefix_4_ ua="na">Yes</DNS_SRV_Auto_Prefix_4_>
<Proxy_Fallback_Intvl_4_ ua="na">3600</Proxy_Fallback_Intvl_4_>
<Proxy_Redundancy_Method_4_ ua="na">Normal</Proxy_Redundancy_Method_4_>
<!--  available options: Normal|Based on SRV Port  -->
<Dual_Registration_4_ ua="na">No</Dual_Registration_4_>
<Auto_Register_When_Failover_4_ ua="na">No</Auto_Register_When_Failover_4_>
<TLS_Name_Validate_4_ ua="na">Yes</TLS_Name_Validate_4_>
 <!--  Subscriber Information  -->
<Display_Name_4_ ua="na"/>
<User_ID_4_ ua="na">4085263128</User_ID_4_>
 <!--  <Password_4_ ua="na">*************</Password_4_>  -->
<Auth_ID_4_ ua="na">AUN3128</Auth_ID_4_>
<Reversed_Auth_Realm_4_ ua="na"/>
<SIP_URI_4_ ua="na"/>
 <!--  XSI Line Service  -->
<XSI_Host_Server_4_ ua="na"/>
<XSI_Authentication_Type_4_ ua="na">Login Credentials</XSI_Authentication_Type_4_>
<!--
 available options: Login Credentials|SIP Credentials
-->
<Login_User_ID_4_ ua="na"/>
```

Profili di configurazione di esempio

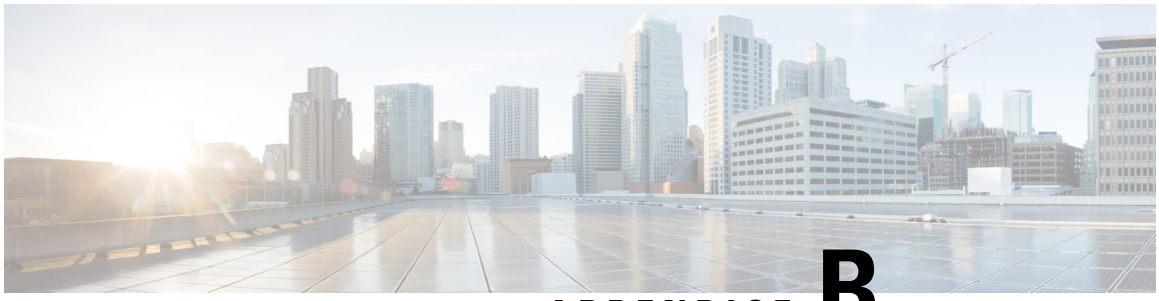
```
 <!--  <Login_Password_4_ ua="na"/>  -->
<Anywhere_Enable_4_ ua="na">No</Anywhere_Enable_4_>
<Block_CID_Enable_4_ ua="na">No</Block_CID_Enable_4_>
<DND_Enable_4_ ua="na">No</DND_Enable_4_>
<CFWD_Enable_4_ ua="na">No</CFWD_Enable_4_>
 <!--  Audio Configuration  -->
<Preferred_Codec_4_ ua="na">G711u</Preferred_Codec_4_>
<!--
 available options: G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Use_Pref_Codec_Only_4_ ua="na">No</Use_Pref_Codec_Only_4_>
<Second_Preferred_Codec_4_ ua="na">Unspecified</Second_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<Third_Preferred_Codec_4_ ua="na">Unspecified</Third_Preferred_Codec_4_>
<!--
 available options: Unspecified|G711u|G711a|G729a|G722|G722.2|iLBC|OPUS
-->
<G711u_Enable_4_ ua="na">Yes</G711u_Enable_4_>
<G711a_Enable_4_ ua="na">Yes</G711a_Enable_4_>
<G729a_Enable_4_ ua="na">Yes</G729a_Enable_4_>
<G722_Enable_4_ ua="na">Yes</G722_Enable_4_>
<G722.2_Enable_4_ ua="na">Yes</G722.2_Enable_4_>
<iLBC_Enable_4_ ua="na">Yes</iLBC_Enable_4_>
<OPUS_Enable_4_ ua="na">Yes</OPUS_Enable_4_>
<Silence_Supp_Enable_4_ ua="na">No</Silence_Supp_Enable_4_>
<DTMF_Tx_Method_4_ ua="na">Auto</DTMF_Tx_Method_4_>
<!--
 available options: InBand|AVT|INFO|Auto|InBand+INFO|AVT+INFO
-->
<Codec_Negotiation_4_ ua="na">Default</Codec_Negotiation_4_>
<!--  available options: Default|List All  -->
<Encryption_Method_4_ ua="na">AES 128</Encryption_Method_4_>
<!--  available options: AES 128|AES 256 GCM  -->
 <!--  Video Configuration  -->
 <!--  Dial Plan  -->
<Dial_Plan_4_ ua="na">
(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)
</Dial_Plan_4_>
<Caller_ID_Map_4_ ua="na"/>
<Enable_URI_Dialing_4_ ua="na">No</Enable_URI_Dialing_4_>
<Emergency_Number_4_ ua="na"/>
 <!--  E911 Geolocation Configuration  -->
<Company_UUID_4_ ua="na"/>
<Primary_Request_URL_4_ ua="na"/>
<Secondary_Request_URL_4_ ua="na"/>
 <!--  Hold Reminder  -->
<Hold_Reminder_Timer ua="rw"/>
<Hold_Reminder_Ring ua="rw">2</Hold_Reminder_Ring>
<!--
 available options: No Ring|1|2|3|4|5|6|7|8|9|10|11|12
-->
 <!--  Call Forward  -->
<Cfwd_Setting ua="rw">Yes</Cfwd_Setting>
<Cfwd_All_Dest ua="rw"/>
<Cfwd_Busy_Dest ua="rw"/>
<Cfwd_No_Ans_Dest ua="rw"/>
<Cfwd_No_Ans_Delay ua="rw">20</Cfwd_No_Ans_Delay>
 <!--  Speed Dial  -->
<Speed_Dial_2_Name ua="rw"/>
<Speed_Dial_2_Number ua="rw"/>
<Speed_Dial_3_Name ua="rw"/>
<Speed_Dial_3_Number ua="rw"/>
```

```
<Speed_Dial_4_Name ua="rw"/>
<Speed_Dial_4_Number ua="rw"/>
<Speed_Dial_5_Name ua="rw"/>
<Speed_Dial_5_Number ua="rw"/>
<Speed_Dial_6_Name ua="rw"/>
<Speed_Dial_6_Number ua="rw"/>
<Speed_Dial_7_Name ua="rw"/>
<Speed_Dial_7_Number ua="rw"/>
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
 <!--  Supplementary Services  -->
<CW_Setting ua="rw">Yes</CW_Setting>
<Block_CID_Setting ua="rw">No</Block_CID_Setting>
<Block_ANC_Setting ua="rw">No</Block_ANC_Setting>
<DND_Setting ua="rw">No</DND_Setting>
<Secure_Call_Setting ua="na">No</Secure_Call_Setting>
<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>
<Preferred_Audio_Device ua="na">None</Preferred_Audio_Device>
<!--  available options: Speaker|Headset|None  -->
<Time_Format ua="na">12hr</Time_Format>
<!--  available options: 12hr|24hr  -->
<Date_Format ua="na">month/day</Date_Format>
<!--  available options: month/day|day/month  -->
<Miss_Call_Shortcut ua="na">No</Miss_Call_Shortcut>
<Handset_LED_Alert ua="rw">Voicemail</Handset_LED_Alert>
<!--
 available options: Voicemail|Voicemail, Missed Call
-->
<Alert_Tone_Off ua="rw">No</Alert_Tone_Off>
<Log_Missed_Calls_for_EXT_1 ua="na">Yes</Log_Missed_Calls_for_EXT_1>
<Log_Missed_Calls_for_EXT_2 ua="na">Yes</Log_Missed_Calls_for_EXT_2>
<Log_Missed_Calls_for_EXT_3 ua="na">Yes</Log_Missed_Calls_for_EXT_3>
<Log_Missed_Calls_for_EXT_4 ua="na">Yes</Log_Missed_Calls_for_EXT_4>
<Shared_Line_DND_Cfwd_Enable ua="na">Yes</Shared_Line_DND_Cfwd_Enable>
 <!--  Camera Profile 1  -->
 <!--  Camera Profile 2  -->
 <!--  Camera Profile 3  -->
 <!--  Camera Profile 4  -->
 <!--  Audio Volume  -->
<Ringer_Volume ua="rw">5</Ringer_Volume>
<Speaker_Volume ua="rw">7</Speaker_Volume>
<Handset_Volume ua="rw">15</Handset_Volume>
<Headset_Volume ua="rw">10</Headset_Volume>
<Ehook_Enable ua="na">No</Ehook_Enable>
 <!--  Audio Compliance  -->
<Compliant_Standard ua="rw">TIA</Compliant_Standard>
<!--  available options: TIA|ETSI  -->
 <!--  Screen  -->
<Screen_Saver_Enable ua="rw">Yes</Screen_Saver_Enable>
<Screen_Saver_Type ua="rw">Clock</Screen_Saver_Type>
<!--  available options: Clock|Download Picture|Logo  -->
<Screen_Saver_Wait ua="rw">60</Screen_Saver_Wait>
<Screen_Saver_Refresh_Period ua="rw">10</Screen_Saver_Refresh_Period>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<!--  available options: Off|10s|20s|30s|Always On  -->
<LCD_Contrast ua="rw">9</LCD_Contrast>
<Boot_Display ua="na">Default</Boot_Display>
<!--
 available options: Default|Download Picture|Logo|Text
-->
<Text_Logo ua="na"/>
<Phone_Background ua="rw">Default</Phone_Background>
```

```
<!--  available options: Default|Logo  -->
<Picture_Download_URL ua="rw"/>
<Logo_URL ua="rw"/>
 <!--  Video Configuration  -->
 <!--  General  -->
<Subscribe_Expires ua="na">1800</Subscribe_Expires>
<Subscribe_Retry_Interval ua="na">30</Subscribe_Retry_Interval>
<Number_of_Units ua="na">0</Number_of_Units>
<!--  available options: 0|1  -->
<Subscribe_Delay ua="na">1</Subscribe_Delay>
<Server_Type ua="na">Broadsoft</Server_Type>
<!--
 available options: Broadsoft|SPA9000|Asterisk|RFC3265_4235|Sylantro
-->
<BLF_List_URI ua="na"/>
<Use_Line_Keys_For_BLF_List ua="na">No</Use_Line_Keys_For_BLF_List>
<Customizable_PLK_Options ua="na">sd;</Customizable_PLK_Options>
<BLF_List ua="na">Show</BLF_List>
<!--  available options: Show|Hide  -->
<Call_Pickup_Audio_Notification ua="na">No</Call_Pickup_Audio_Notification>
<Attendant_Console_LCD_Contrast ua="na">8</Attendant_Console_LCD_Contrast>
<BXfer_To_Starcode_Enable ua="na">No</BXfer_To_Starcode_Enable>
<BXfer_On_Speed_Dial_Enable ua="na">No</BXfer_On_Speed_Dial_Enable>
<BXfer_To_Remote_Party_Number_Enable ua="na">No</BXfer_To_Remote_Party_Number_Enable>
<BLF_Label_Display_Mode ua="na">Both</BLF_Label_Display_Mode>
<!--  available options: Name|Ext|Both  -->
<Wake_up_phone_screen_when_BLF_pickup_is_ringing
ua="na">No</Wake_up_phone_screen_when_BLF_pickup_is_ringing>
 <!--  Unit 1  -->
<Unit_1_Key_1_ ua="na"/>
<Unit_1_Key_2_ ua="na"/>
<Unit_1_Key_3_ ua="na"/>
<Unit_1_Key_4_ ua="na"/>
<Unit_1_Key_5_ ua="na"/>
<Unit_1_Key_6_ ua="na"/>
<Unit_1_Key_7_ ua="na"/>
<Unit_1_Key_8_ ua="na"/>
<Unit_1_Key_9_ ua="na"/>
<Unit_1_Key_10_ ua="na"/>
<Unit_1_Key_11_ ua="na"/>
<Unit_1_Key_12_ ua="na"/>
<Unit_1_Key_13_ ua="na"/>
<Unit_1_Key_14_ ua="na"/>
<Unit_1_Key_15_ ua="na"/>
<Unit_1_Key_16_ ua="na"/>
<Unit_1_Key_17_ ua="na"/>
<Unit_1_Key_18_ ua="na"/>
<Unit_1_Key_19_ ua="na"/>
<Unit_1_Key_20_ ua="na"/>
<Unit_1_Key_21_ ua="na"/>
<Unit_1_Key_22_ ua="na"/>
<Unit_1_Key_23_ ua="na"/>
<Unit_1_Key_24_ ua="na"/>
<Unit_1_Key_25_ ua="na"/>
<Unit_1_Key_26_ ua="na"/>
<Unit_1_Key_27_ ua="na"/>
<Unit_1_Key_28_ ua="na"/>
 <!--  TR-069  -->
<Enable_TR-069 ua="na">No</Enable_TR-069>
<ACS_URL ua="na"/>
<ACS_Username ua="na"/>
 <!--  <ACS_Password ua="na"/>  -->
<Connection_Request_Username ua="na"/>
 <!--  <Connection_Request_Password ua="na"/>  -->
```

```
<Periodic_Inform_Interval ua="na">20</Periodic_Inform_Interval>
<Periodic_Inform_Enable ua="na">Yes</Periodic_Inform_Enable>
<TR-069_Traceability ua="na">No</TR-069_Traceability>
<CWMP_V1.2_Support ua="na">Yes</CWMP_V1.2_Support>
<TR-069_VoiceObject_Init ua="na">Yes</TR-069_VoiceObject_Init>
<TR-069_DHCPOption_Init ua="na">Yes</TR-069_DHCPOption_Init>
<TR-069_Fallback_Support ua="na">No</TR-069_Fallback_Support>
<BACKUP_ACS_URL ua="na"/>
<BACKUP_ACS_User ua="na"/>
 <!--  <BACKUP_ACS_Password ua="na"/>  -->
</flat-profile>
```

Profili di configurazione di esempio



APPENDICE B

Acronimi

Acronimi

AC	Corrente alternata
ACS	Access Control Server
A/D	Convertitore da analogo a digitale
AES	Advanced Encryption Standard
ANC	Chiamata anonima
AP	Access Point
ASCII	American Standard Code for Information Interchange
B2BUA	Torna ad agente utente
CLO	Indicatore di stato
Bool	Valori booleani. Specificati come Sì/No o 1 e 0 nel profilo.
BootP	Protocollo Bootstrap
CA	Autorità certificativa
CAS	Segnale di avviso CPE
CDP	Cisco Discovery Protocol
CDR	Cartellino chiamata
CGI	Computer-Generated Imagery
CID	ID chiamante
CIDCW	ID chiamante chiamata in attesa

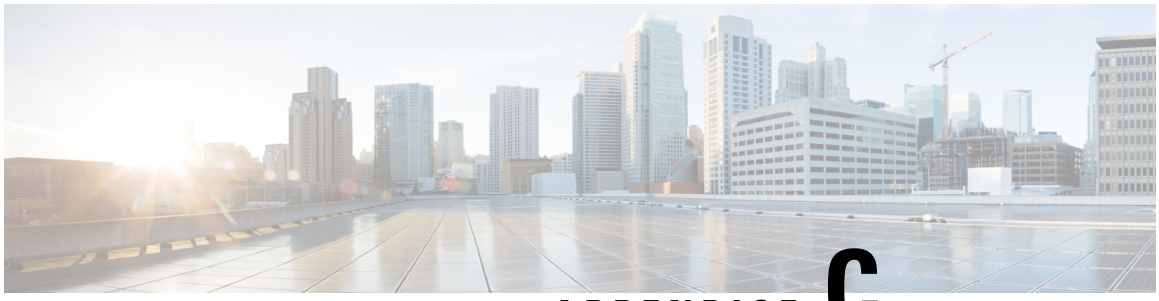
CNG	Generatore del rumore di comfort
CPC	Controllo identificativo chiamante
CPE	Customer Premises Equipment (Attrezzatura presso sede del cliente)
CSV	Valori separati da virgola
CWCID	ID chiamante chiamata in attesa
CWT	Call Waiting Tone (Segnale di chiamata in attesa)
D/A	Convertitore da analogico a digitale
dB	Decibel
dBm	dB rispetto a milliwatt 1
DHCP	DHCP (Dynamic Host Configuration Protocol)
Non disturbare.	Non disturbare
DNS	Domain Name System
DoS	Denial of Service
DRAM	Memoria dinamica di accesso casuale
DSL	Linea utente digitale
DSP	Digital Signal Processor
DST	Ora legale
DTAS	Terminale avviso segnale dati (come CAS)
DTMF	Frequenza multipla segnale doppio
FQDN	Nome di dominio completo
FSK	Uso tastiera per spostamento frequenza
FW	Firmware
FXS	Foreign eXchange Station
GMT	Greenwich Mean Time
GW	Gateway
HTML	Hypertext Markup Language
HTTP	HTTP (Hypertext Transfer Protocol)
HTTPS	HTTP su SSL

ICMP	ICMP (Internet Control Message Protocol)
IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	IP (Internet Protocol)
IPv4	Internet Protocol versione 4
IPv6	Internet Protocol versione 6
ISP	Provider di servizi Internet
ITSP	Provider di servizi di telefonia e Internet
ITU	International Telecommunication Union
IVR	Interactive Voice Response
LAN	LAN (Local Area Network)
LBR	Velocità in bit bassa
LBRC	Codec con velocità in bit bassa
LCD	Liquid Crystal Display; noto anche come schermo
LDAP	Lightweight Directory Access Protocol
LED	Light-Emiting Diode
Indirizzo MAC	Indirizzo per il controllo degli accessi ai supporti (Media Access Control)
MC	Mini certificato
MGCP	Media Gateway Control Protocol
Musica di attesa (MOH)	Musica in attesa
MOS	Mean Opinion Score (da 1 a 5, con 5 come valore elevato migliore)
MPP	Telefoni multipiattaforma
ms	Millisecondo
MSA	Adattatore sorgente musica
MWI	Indicazione di messaggio in attesa
NAT	NAT (Network Address Translation)
NPS	Normal Provisioning Server
NTP	NTP (Network Time Protocol)

OOB	Fuori banda
OSI	Intervallo di commutazione aperto
PBX	Centralino telefonico
PCB	Circuito stampato
PoE	Power over Ethernet (PoE)
PR	Inversione di polarità
PS	Server di provisioning
PSQM	Misurazione di qualità vocale percettiva (da 1 a 5, con 1 come valore migliore)
PSTN	Public Switched Telephone Network
QoS	Qualità del servizio
CM	Rimuovi personalizzazione
REQT	(SIP) Messaggio di richiesta
RESP	(SIP) Messaggio di risposta
RSC	(SIP) Codice di stato risposta, ad esempio 404, 302, 600
RTP	Real Time Protocol
RTT	Tempo di round trip
SAS	Streaming Audio Server
SDP	Session Description Protocol
SDRAM	DRAM sincrona
sec.	Secondi
SIP	Session Initiation Protocol
SLA	Identificativo di linea condivisa
SLIC	Subscriber Line Interface Circuit
SP	Provider di servizi
SSL	Secure Socket Layer
STUN	Session Traversal UDP per NAT
TCP	TCP (Transmission Control Protocol)
TFTP	TFTP (Trivial File Transfer Protocol)
TLS	Transport Layer Security

TTL	Durata
ToS	Tipo di servizio
UA	Agente utente
UC	Micro-controller
UDP	Protocollo UDP (User Datagram Protocol)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Orario coordinato universale
VAR	Value Added Reseller
VLAN	LAN voce
VM	Segreteria telefonica
VMWI	Indicatore/Indicazione di messaggio in attesa
VoIP	Protocollo Internet su voce
VQ	Qualità della voce
WAN	WAN (Wide Area Network)
XML	Extensible Markup Language

Acronimi



APPENDICE C

Documentazione correlata

Documentazione correlata

Utilizzare le sezioni indicate di seguito per le relative informazioni.

Documentazione di Cisco IP Phone serie 6800

Consultare le pubblicazioni specifiche della propria lingua, del modello del telefono e della versione firmware dei telefoni multipiattaforma utilizzando il seguente URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/tsd-products-support-series-home.html

Policy di supporto per il firmware del telefono Cisco IP Phone

Per informazioni sulla policy di supporto per i telefoni, vedere https://cisco.com/go/phonefirmwaresupport.