Guia de aprovisionamento para telefones multiplataforma Cisco IP Phone 6800 Series

Primeira publicação: 2017-11-22

Última modificação: 2019-01-30

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.

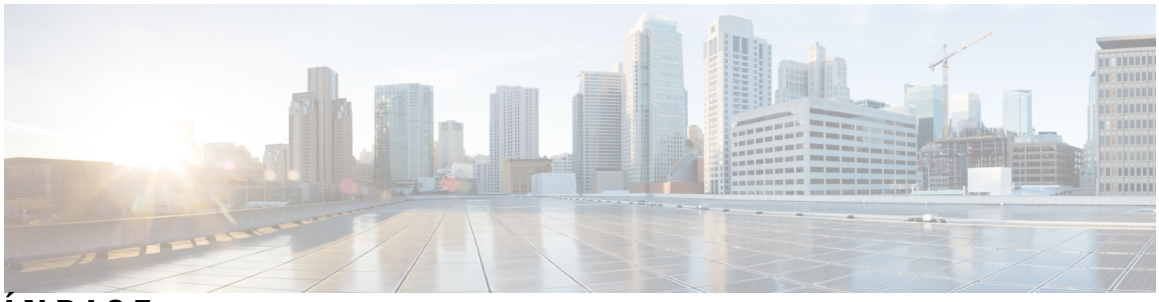
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY 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 e o logótipo da Cisco são marcas comerciais ou marcas comerciais registadas da Cisco e/ou das respetivas empresas afiliadas nos EUA e noutros países. Para ver uma lista de marcas comerciais da Cisco, aceda a este URL: www.cisco.com go trademarks. As marcas comerciais de terceiros mencionadas são propriedade dos respetivos proprietários. A utilização da palavra parceiro não implica uma relação de parceria entre a Cisco e qualquer outra empresa. (1721R)



ÍNDICE

CAPÍTULO 1

Implementação e aprovisionamento

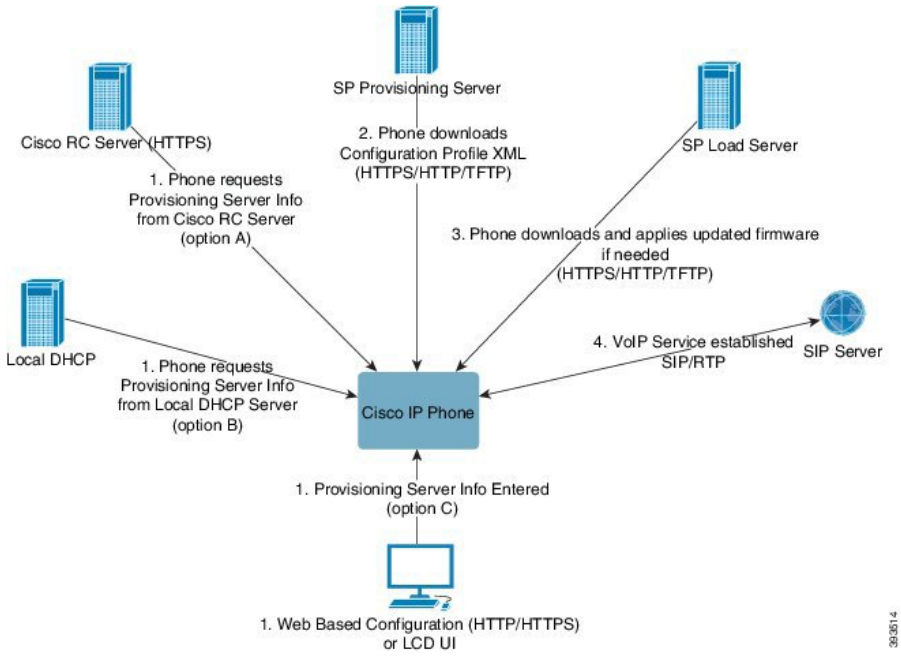
Descrição geral de aprovisionamento

Os Cisco IP Phones destinam-se a implementações de grandes volumes por parte de provedores de serviços Voice-over-IP (VoIP) a clientes em ambientes residenciais, comerciais ou empresariais. Assim, o aprovisionamento do telefone com configuração e gestão remota assegura o funcionamento adequado do telefone no local do cliente.

A Cisco suporta a configuração personalizada e contínua das funcionalidades do telefone utilizando:

- Controlo remoto fiável do telefone.
- Encriptação de comunicação que controla o telefone.
- Associação de conta do telefone otimizada.

É possível aprovisionar os telefones para transferirem perfis de configuração ou atualizarem um firmware de um servidor remoto. As transferências podem ocorrer quando os telefones estão ligados a uma rede, quando estão ligados e com intervalos definidos. Normalmente o aprovisionamento faz parte das implementações de grandes volumes de VoIP comuns aos provedores de serviços. Os perfis de configuração ou firmware atualizado são transferidos para o dispositivo utilizando TFTP, HTTP ou HTTPS.



Num alto nível, o processo de aprovisionamento de telefone é o seguinte:

1. Se o telefone não estiver configurado, as informações do servidor de aprovisionamento são aplicadas ao telefone utilizando uma das seguintes opções:
   - **A**–Transferidos do servidor de personalização remota (RC) Enablement Data Orchestration System (EDOS) da Cisco com HTTPS.
   - **B**– Consultados a partir de um servidor DHCP local.
   - **C**– Inseridos manualmente com o utilitário de configuração de telefones Cisco baseado na Web ou a IU do telefone.
2. O telefone transfere as informações do servidor de aprovisionamento e se aplica a configuração XML com os protocolos HTTPS, HTTP ou TFTP.
3. O telefone transfere e aplica o firmware atualizado, se necessário, com HTTPS, HTTP ou TFTP.
4. O serviço de VoIP é estabelecido com o firmware e configuração especificados.

Os provedores de serviços de VoIP pretendem implementar muitos telefones em clientes residenciais e de pequenos negócios. Em ou ambientes comerciais e empresariais, os telefones podem servir como nós terminais. Os provedores distribuem largamente estes dispositivos através da Internet, ligados através de routers e firewalls às instalações dos clientes.

O telefone pode ser utilizado como uma extensão remota do equipamento de back-end do provedor de serviços. A configuração e gestão remota garantem o funcionamento adequado do telefone nas instalações do cliente.

Aprovisionamento TR69

O Cisco IP Phone ajuda o administrador a configurar os parâmetros TR69 com a IU da Web. Para obter informações relacionadas com os parâmetros, incluindo uma comparação dos parâmetros XML e TR69, consulte o Guia de Administração da série de telefones correspondente.

Os telefones suportam deteção Auto Configuration Server (ACS) das Opções de DHCP 43, 60 e 125.

- Opção 43 – informações específicas do vendedor para o URL do ACS.
- Opção 60 – identificador de classe do vendedor, para o telefone se identificar com `dslforum.org` ao ACS.
- Opção 125 – informações específicas do vendedor para a associação do gateway.

Métodos RPC

Métodos RPC suportados

Os telefones suportam apenas um conjunto limitado de métodos de Chamada de procedimento remoto (RPC):

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download: Método RPC de transferência, os tipos de ficheiro suportados são:
    - Imagem de atualização do firmware
    - Ficheiro de configuração do fornecedor
    - Ficheiro personalizado de Autoridade de Certificação
- Transferência concluída

Tipos de evento suportados

Os telefones suportam tipos de evento com base nas funcionalidades e métodos suportados. São suportados os seguintes tipos de evento:

- Inicialização
- Arranque
- alteração de valor
- pedido de ligação
- Periódico
- Transferência concluída
- Transferência M
- Reinicialização M

Comportamento do telefone durante períodos de congestionamento da rede

- Tarefas administrativas tais como leituras de portas internas ou verificações de segurança
- Ataques que ocorram na rede, por exemplo, um ataque de negação de serviço

Implementação

Os Cisco IP Phones oferecem mecanismos convenientes de aprovisionamento, com base nestes modelos de implementação:

- Distribuição em massa — o provedor de serviços adquire Cisco IP Phones em massa e efetua o respetivo pré-aprovisionamento internamente ou adquire unidades de personalização remota à Cisco. Em seguida, os dispositivos são entregues aos clientes como parte de um contrato de serviço de VoIP.
- Distribuição a retalho — O cliente adquire o Cisco IP Phone numa loja de venda a retalho e pede um de serviço de VoIP ao provedor de serviços. O provedor de serviços deve depois suportar a configuração remota segura do dispositivo.

Distribuição em massa

Neste modelo, o provedor de serviços atribui telefones aos respetivos clientes como parte de um contrato de serviço de VoIP. Os dispositivos são unidades de personalização remota ou pré-aprovisionados internamente.

A Cisco pré-aprovisiona unidades de personalização remota para ressincronizar com um servidor Cisco que transfere as atualizações de firmware e de perfil do dispositivo.

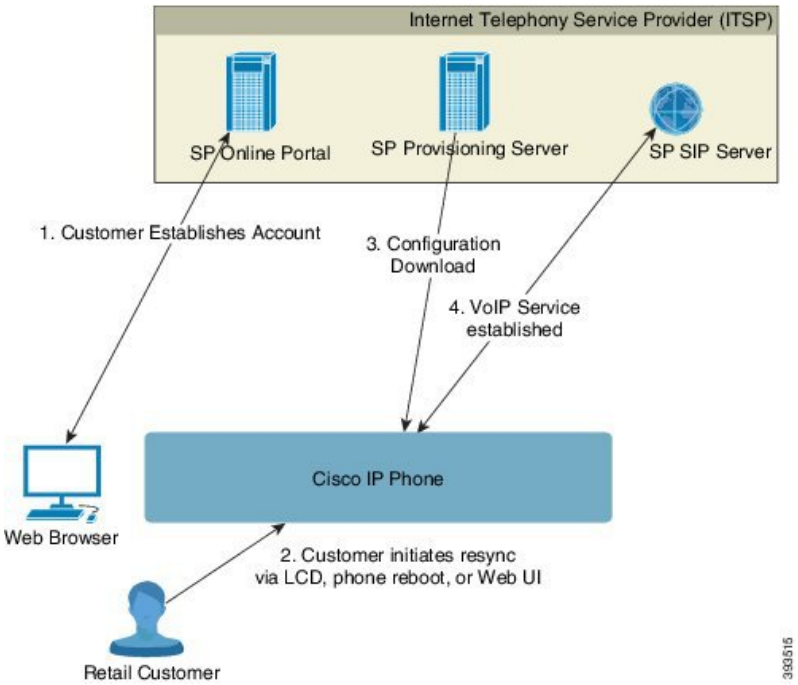
Um provedor de serviços pode pré-aprovisionar telefones com os parâmetros pretendidos, incluindo os parâmetros que controlam a ressincronização, através de vários métodos:

- Internamente, com DHCP e TFTP
- Remotamente, com TFTP, HTTP ou HTTPS
- Uma combinação de aprovisionamento interno e remoto

Distribuição a retalho

Num modelo de distribuição a retalho, um cliente adquire um telefone e subscreve um serviço específico. O provedor de serviços de telefonia de Internet (ITSP) configura e mantém um servidor de aprovisionamento, e pré-aprovisiona o telefone para ressincronizar com o servidor do provedor de serviços.

Figura 1: Distribuição a retalho



O telefone inclui o utilitário de configuração baseado na web que apresenta a configuração interna e aceita novos valores de parâmetros de configuração. O servidor também aceita uma sintaxe de comando URL especial para realizar operações remotas de atualização de firmware e ressincronização do perfil.

O cliente inicia sessão no serviço e estabelece uma conta de VoIP, possivelmente através de um portal on-line, e associa o dispositivo à conta de serviço atribuída. O telefone não aprovisionado recebe instruções para ressincronizar com um servidor de aprovisionamento específico através de um comando de URL de ressincronização. O comando de URL normalmente inclui um número de ID ou código alfanumérico de cliente da conta para associar exclusivamente o dispositivo à nova conta.

No exemplo que se segue, um dispositivo no endereço IP atribuído por DHCP 192.168.1.102 recebe instruções para se aprovisionar ao serviço de SuperVoIP:

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

Neste exemplo, 1234abcd é o número de ID do cliente da nova conta. O servidor de aprovisionamento remoto associa o telefone que executa o pedido de ressincronização com a nova conta, com base no URL e no ID do cliente fornecido. Através da operação de ressincronização inicial, o telefone é configurado num só passo. O telefone é automaticamente direcionado para ressincronizar com um URL permanente no servidor. Por exemplo:

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

Tanto para acesso inicial como para acesso permanente, o servidor de aprovisionamento depende o certificado do cliente do telefone para autenticação. O servidor de aprovisionamento fornece valores de parâmetros de configuração corretos com base na conta de serviço associada.

Quando o dispositivo está ligado ou tiver decorrido um tempo especificado, o telefone ressincroniza e transfere os parâmetros mais recentes. Estes parâmetros podem tratar de objetivos como configurar um grupo de busca, definir números de marcação rápida e limitar as funcionalidades que um utilizador pode modificar.

Tópicos relacionados

Pré-aprovisionamento interno do dispositivo, na página 41

Processo de ressincronização

O firmware para cada telefone inclui um servidor Web de administração que aceita novos valores de parâmetros de configuração. O telefone pode receber instruções para ressincronizar a configuração após a reinicialização, ou em intervalos agendados com um servidor de aprovisionamento especificado através de comando de URL de ressincronização no perfil de dispositivo.

Por predefinição, o servidor Web está ativado. Para desativar ou ativar o servidor Web, utilize o comando de URL ressincronização.

Se necessário, pode ser pedida uma ressincronização imediata através de um URL de ação "ressincronização". O comando de URL para ressincronização pode incluir um número de ID da conta do cliente ou um código alfanumérico para associar exclusivamente o dispositivo à conta do utilizador.

Exemplo

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

Neste exemplo, um dispositivo no endereço IP atribuído por DHCP 192.168.1.102 recebe instruções para se aprovisionar ao serviço de SuperVoIP em prov.supervoip.com. O número de ID do cliente para a nova conta é 1234abcd. O servidor de aprovisionamento remoto associa o telefone que executa o pedido de ressincronização com a conta, com base no URL e ID do cliente.

Através da operação de ressincronização inicial, o telefone é configurado num só passo. O telefone é automaticamente direcionado para ressincronizar com um URL permanente no servidor.

Tanto para acesso inicial como para acesso permanente, o servidor de aprovisionamento depende o certificado do cliente para autenticação. O servidor fornece valores de parâmetros de configuração com base na conta de serviço associada.

Aprovisionamento

Um telefone pode ser configurado para ressincronizar o respetivo estado de configuração interno para corresponder a um perfil remoto periodicamente e ao ligar. O telefone entra em contacto com um servidor de aprovisionamento normal (NPS) ou um servidor de controlo de acesso (ACS).

Por predefinição, só é feita uma tentativa de ressincronização de perfil quando o telefone está inativo. Esta prática impede uma atualização acione uma reinicialização do software e interrompa uma chamada. Se forem necessárias atualizações intermédias para alcançar um estado atual de atualização de uma versão antiga, a lógica de atualização pode automatizar atualizações em várias fases.

Servidor de aprovisionamento normal

O servidor de aprovisionamento normal (NPS) pode ser um servidor TFTP, HTTP ou HTTPS. Uma atualização de firmware remoto é atingida com TFTP ou HTTP, ou HTTPS, porque o firmware não contém informações confidenciais.

Embora se recomende HTTPS, a comunicação com o NPS não exige a utilização de um protocolo seguro, porque o perfil atualizado pode ser encriptado por uma chave secreta partilhada. Para obter mais informações sobre a utilização de HTTPS, consulte Encriptação de comunicação, na página 9. O primeiro aprovisionamento seguro é fornecido por um mecanismo que utiliza a funcionalidade SSL. Um telefone não aprovisionado pode receber um perfil encriptado com chave simétrica de 256 bits direcionada para esse dispositivo.

Controlo de acesso de configuração

O firmware do telefone fornece mecanismos para restringir o acesso de utilizadores finais a alguns parâmetros. O firmware fornece privilégios específicos para iniciar sessão numa conta **Admin** ou numa conta de **utilizador**. Cada uma pode ser protegida por palavra-passe independentemente.

- Conta Admin - dá ao provedor de serviços acesso total a todos parâmetros do servidor Web de administração.
- Conta de utilizador - permite ao utilizador configurar um subconjunto de parâmetros de servidor Web de administração.

O provedor de serviços pode restringir a conta de utilizador no perfil de aprovisionamento das seguintes maneiras:

- Indicando que parâmetros de configuração estão disponíveis para a conta de utilizador ao criar a configuração.
- Desativando o acesso do utilizador ao servidor da Web de administração.
- Desativando o acesso do utilizador à interface do utilizador do LCD.
- Ignorar o **definir palavra-passe** ecrã para o utilizador.
- Restringindo os domínios de Internet a que o dispositivo acede para ressicronizações, atualizações e registo SIP para a linha 1.

Tópicos relacionados

Propriedades do marcador de elemento, na página 14
Controlo de acesso, na página 16

Aceder à página da Web do telefone

Aceda à página da web do telefone a partir de um web browser num computador que se consiga ligar ao telefone na sub-rede.

Se o seu provedor de serviços tiver desativado o acesso ao utilitário de configuração, contacte o provedor de serviços antes de continuar.

Procedure

Passo 1 Certifique-se de que o computador consegue comunicar com o telefone. Não deve haver VPN em utilização.

Passo 2 Inicie um web browser.

Passo 3 Introduza o endereço IP do telefone na barra de endereço do web browser.

- Acesso do utilizador: **`http://<endereço ip>/user`**
- Acesso Admin: **`http://<endereço ip>/admin/advanced`**
- Acesso Admin: **`http://<endereço ip>`**, clique em **Início de sessão do administrador** e clique em **Avançado**

Por exemplo, `http://10.64.84.147/admin`

Permitir o acesso à Web do Cisco IP Phone

Para ver os parâmetros de telefone, ative o perfil de configuração. Para fazer alterações em qualquer um dos parâmetros, é necessário ter capacidade de alterar o perfil de configuração. O administrador do sistema pode ter desativado a opção de telefone para fazer a interface de usuário do telefone da web visíveis ou que pode ser gravado.

Para mais informações, consulte o *Guia de aprovisionamento para telefones multiplataforma Cisco IP Phone 6800 Series*.

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Clique em **Voz** > **Sistema**.

Passo 2 Na secção **Configuração do sistema**, defina **Ativar servidor Web** para **Sim**.

Passo 3 Para atualizar o perfil de configuração, clique em **Enviar todas as alterações** depois de modificar os campos na interface de utilizador da Web do telefone.

O telefone é reinicializado e as alterações são aplicadas.

Passo 4 Para limpar todas as alterações feitas durante a sessão atual (ou depois de ter clicado pela última vez em **Enviar todas as alterações**), clique em **Desfazer todas as alterações**. Os valores regressam às respetivas configurações anteriores.

Encriptação de comunicação

Os parâmetros de configuração comunicados ao dispositivo podem conter códigos de autorização ou outras informações que protegem o sistema de acessos não autorizados. É do interesse do provedor de serviços impedir a atividade de clientes não autorizados. É do interesse do cliente impedir a utilização não autorizada da conta. O provedor de serviços pode encriptar as comunicações do perfil de configuração entre o servidor de aprovisionamento e o dispositivo, além de limitar o acesso ao servidor Web da administração.

Práticas de aprovisionamento do telefone

Normalmente, o Cisco IP Phone é configurado para aprovisionamento na primeira ligação à rede. O telefone também é aprovisionado em intervalos agendados, definidos quando o provedor de serviços ou o VAR pré-aprovisiona (configura) o telefone. Os provedores de serviços podem autorizar VARs ou utilizadores avançados para aprovisionar manualmente o telefone através do teclado do telefone. Também é possível configurar o aprovisionamento com a IU Web do telefone.

Verifique o **Estado** > **Estado do telefone** > **Aprovisionamento** a partir do da IU do LCD do telefone, ou o Estado de aprovisionamento no separador **Estado** do Utilitário de configuração com base na web.

Tópicos relacionados

Aprovisionamento manual de um telefone a partir do teclado, na página 9

Aprovisionamento manual de um telefone a partir do teclado

Procedure

Passo 1 Prima **Aplicações**  .

Passo 2 Selecione **Administração do dispositivo** > **Regra do perfil**.

Passo 3 Introduza a regra do perfil utilizando o seguinte formato:

```
protocolo://servidor[:porta]/nomecaminho_perfil
```

Por exemplo:

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

Se não for especificado um protocolo, é utilizado por predefinição TFTP. Se não for especificado um nome de servidor, o anfitrião que pede o URL é utilizado como nome do servidor. Se não for especificada uma porta, é utilizada a porta predefinida (69 para TFTP, 80 para HTTP ou 443 para HTTPS).

Passo 4 Prima **Ressinc.**

Tópicos relacionados

Práticas de aprovisionamento do telefone, na página 9

Partilhar firmware par a par

A partilha de firmware par a par (PFS) é um modelo de distribuição de firmware que permite a um telefone Cisco IP encontrar outros telefones do mesmo modelo ou série na sub-rede e partilhar ficheiros de firmware

atualizados quando é necessário atualizar vários telefones em simultâneo. O PFS utiliza o protocolo CPPDP (Cisco Peer-to-Peer-Distribution Protocol) que é um protocolo propriedade da Cisco. Com o CPPDP, todos os dispositivos na sub-rede formam uma hierarquia par a par e, em seguida, copiam o firmware ou os outros ficheiros de dispositivos pares para os dispositivos vizinhos. Para otimizar atualizações de firmware, um telefone raiz transfere a imagem de firmware do servidor de carregamento e, em seguida, transfere o firmware para outros telefones na sub-rede utilizando ligações TCP.

Partilha de firmware par a par:

- Limita o congestionamento em transferências TFTP para servidores de carregamento de remoção centralizada.
- Elimina a necessidade de controlar manualmente atualizações de firmware.
- Reduz o tempo de inatividade do telefone durante atualizações quando grandes números de telefones são repostos em simultâneo.

Nota

- A partilha de firmware par a par não funciona a menos que vários telefones estejam definidos para serem atualizados em simultâneo. Quando uma NOTIFICAÇÃO é enviada com Event:resync, inicia uma ressincronização no telefone. Exemplo de um xml que pode conter as configurações para iniciar a atualização:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Ao definir o servidor de registo da partilha de firmware par a par para um endereço IP e porta, os registos específicos do PFS são enviados para esse servidor como mensagens UDP. Esta definição tem de ser efetuada em cada telefone. Em seguida, é possível utilizar as mensagens de sessão quando problemas relacionados para essa opção de resolução de problemas.

Peer_Firmware_Sharing_Log_Server especifica o nome de anfitrião do servidor UDP remoto de syslog e a porta. A predefinição da porta do syslog é 514.

Por exemplo:

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

Para utilizar esta funcionalidade, ative o FPS nos telefones.

Ignorar o ecrã Definir palavra-passe

Pode ignorar o ecrã **Definir palavra-passe** do telefone no primeiro arranque ou após a reposição de fábrica, com base nestas ações de aprovisionamento:

- Configuração de DHCP
- Configuração de EDOS
- Configuração da palavra-passe do utilizador utilizando o ficheiro de configuração XML no telefone.

Tabela 1: Ações de aprovisionamento que determinam se o ecrã Definir palavra-passe é apresentado

DHCP configurado	EDOS configurado	Palavra-passe de utilizador configurada	Ignorar ecrã Definir palavra-passe
Sim	n/a	Sim	Sim
Sim	n/a	Não	**Não**
Não	Sim	Sim	Sim
Não	Sim	Não	**Não**
Não	Não	n/a	**Não**

Procedure

Passo 1 Edite o ficheiro `config.xml` do telefone num editor de texto ou XML.

Passo 2 Insira a etiqueta **`<User_Password>`** utilizando uma destas opções.

- **Sem palavra-passe (etiqueta de início e de fim)**–**`<User_Password></User_Password>`**
- **Valor da palavra-passe (4 a 127 caracteres)**–**`<User_Password ua="rw">abc123</User_Password>`**
- **Sem palavra-passe (etiqueta de início apenas)**–**`<User_Password />`**

Passo 3 Guarde as alterações ao ficheiro `config`.

CAPÍTULO 2

Aprovisionamento de scripts

Aprovisionamento de scripts

O telefone aceita configuração num formato XML.

Para obter informações detalhadas sobre o telefone, consulte o guia de administração do seu dispositivo específico. Cada guia descreve os parâmetros que podem ser configurados através do servidor Web da administração.

Formatos de perfil de configuração

O perfil de configuração define os valores de parâmetros para o telefone.

O formato XML do perfil de configuração utiliza ferramentas de criação XML padrão para compilar os parâmetros e os valores.

Nota Só é suportado o conjunto de caracteres UTF-8. Se modificar o perfil num editor, não altere o formato de codificação; caso contrário, o telefone não consegue reconhecer o ficheiro.

Cada telefone tem um conjunto de recursos diferentes e, por conseguinte, um conjunto de parâmetros diferentes.

Perfil do formato XML (XML)

O perfil de formato aberto é um ficheiro de texto com sintaxe semelhante a XML numa hierarquia de elementos, com atributos e valores de elementos. Este formato permite-lhe utilizar ferramentas padrão para criar o ficheiro de configuração. Um ficheiro de configuração neste formato pode ser enviado do servidor de aprovisionamento

para o telefone durante uma operação de ressincronização. O ficheiro pode ser enviado sem compilação como objeto binário.

O telefone pode aceitar formatos de configuração gerados por ferramentas padrão. Esta funcionalidade facilita o desenvolvimento de software de servidor de aprovisionamento back-end que gera perfis de configuração a partir de bases de dados existentes.

Para proteger informações confidenciais no perfil de configuração, o servidor de aprovisionamento fornece este tipo de ficheiro ao telefone através de um canal protegido por TLS. Opcionalmente, o ficheiro pode ser comprimido com o algoritmo deflate gzip (RFC1951).

O ficheiro pode ser encriptado com um dos seguintes métodos de encriptação:

- Encriptação AES-256-CBC
- Encriptação de conteúdo HTTP baseada em RFC-8188 com cifragem AES-128-GCM

Exemplo: Formato de perfil aberto

```
<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>
```

O marcador de elemento <flat-profile> engloba todos os elementos de parâmetro reconhecidos pelo telefone.

Tópicos relacionados

Compressão e encriptação de perfil aberto (XML), na página 18

Componentes do ficheiro de configuração

Um ficheiro de configuração pode incluir os seguintes componentes:

- Marcadores de elemento
- Atributos
- Parâmetros
- Funcionalidades de formatação
- Comentários XML

Propriedades do marcador de elemento

- O formato de aprovisionamento XML e a interface de utilizador da Web permitem a configuração das mesmas definições. O nome do marcador XML e os nomes de campos na interface de utilizador da Web são semelhantes mas variam devido a restrições de nome do elemento XML. Por exemplo, sublinhados (_) em vez de " ".
- O telefone reconhece os elementos com nomes de parâmetros adequados encapsulados no elemento especial <flat-profile>.

- Os nomes de elemento são colocados entre parênteses angulares.
- A maioria dos nomes de elemento são semelhantes aos nomes de campos nas páginas da Web de administração para o dispositivo, com as seguintes modificações:
  - Os nomes de elemento não podem incluir espaços nem caracteres especiais. Para derivar o nome do elemento do nome do campo de administração web, substitua para cada espaço ou carácter especial `[`, `]`, `(`, `)` ou `/` por um carácter sublinhado.

    Exemplo: O elemento <Resync_On_Reset> representa o campo **Ressincronizar ao repor**.
  - Cada nome de elemento deve ser exclusivo. Nas páginas da Web da administração, os mesmos campos podem aparecer em várias páginas da Web, como as páginas Linha, Utilizador e Extensão. Anexe `[n]` ao nome do elemento para indicar o número apresentado no separador da página.

    Exemplo: O elemento <Dial_Plan_1_> representa o **Plano de marcação** para a Linha 1.
- Cada marcador de elemento de abertura deve ter um marcador de elemento de encerramento correspondente. Por exemplo:

```
<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>
```

- Os marcadores de elemento são sensíveis a maiúsculas e minúsculas.
- São permitidos marcadores de elemento vazios, que serão interpretados como uma configuração do valor para vazio. Introduza o marcador do elemento de abertura sem um marcador de elemento correspondente, e introduza um espaço e uma barra antes do parênteses angular de encerramento (>). Neste exemplo, a Regra de perfil B está vazia:

```
<Profile_Rule_B />
```

- É possível utilizar um marcador de elemento vazio para impedir a substituição de quaisquer valores fornecidos pelo utilizador durante uma operação de ressincronização. No exemplo que se segue, as configurações de marcação rápida do utilizador ficam inalteradas:

```
<flat-profile>
<Speed_Dial_2_2_ ua=”rw”/>
<Speed_Dial_3_2_ ua=”rw”/>
<Speed_Dial_4_2_ ua=”rw”/>
<Speed_Dial_5_2_ ua=”rw”/>
<Speed_Dial_6_2_ ua=”rw”/>
<Speed_Dial_7_2_ ua=”rw”/>
<Speed_Dial_8_2_ ua=”rw”/>
<Speed_Dial_9_2_ ua=”rw”/>
</flat-profile>
```

- Utilize um valor vazio para definir o parâmetro correspondente para uma cadeia de caracteres vazia. Introduza um elemento de abertura encerramento sem qualquer valor entre eles. No exemplo a seguir, o parâmetro GPP_A é definido como uma cadeia de caracteres vazia.

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

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

- Os nomes de elemento não reconhecidos são ignorados.

Tópicos relacionados

Controlo de acesso de configuração, na página 7

Atributo de acesso do utilizador

É possível utilizar os controlos de atributo de acesso do utilizador (**ua**) para alterar o acesso pela conta de utilizador. Se o atributo **ua** não for especificado, mantém-se a configuração de acesso do utilizador existente. Este atributo não afeta o acesso da conta Admin.

O atributo **ua**, se presente, deve ter um dos seguintes valores:

- na - sem acesso
- ro - só de leitura
- rw - leitura e escrita

O exemplo a seguir ilustra o atributo **ua**:

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

O valor da opção **ua** deve estar entre aspas.

Controlo de acesso

Se o parâmetro <Phone-UI-User-Mode> estiver ativado, a GUI do telefone honra o atributo de acesso do utilizador dos parâmetros relevantes quando a GUI apresentar um item de menu.

Para entradas de menu associadas a um só parâmetro de configuração:

- Aprovisionar o parâmetro com o atributo “ua=na” (“ua” significa “acesso do utilizador”) faz com que a entrada desapareça.
- Aprovisionar o parâmetro com o atributo “ua=ro” faz com que a entrada seja só de leitura e não editável.

Para entradas de menu associadas a vários parâmetros de configuração:

- Aprovisionar todos os parâmetros em questão com o atributo “ua=na” faz com que as entradas desapareçam.

Tópicos relacionados

Controlo de acesso de configuração, na página 7

Propriedades de parâmetros

Estas propriedades aplicam-se aos parâmetros:

- Quaisquer parâmetros não especificados por um perfil são deixados inalterados no telefone.

- Os parâmetros não reconhecidos são ignorados.
- Se o perfil de formato aberto contiver várias ocorrências do mesmo marcador de parâmetro, as últimas ocorrências substituem todas as anteriores. Para evitar a sobreposição inadvertida de valores de configuração de um parâmetro, recomendamos que cada perfil especifique no máximo uma instância de um parâmetro.
- O último perfil processado tem precedência. Se vários perfis especificarem o mesmo parâmetro de configuração, o valor do perfil mais recente tem precedência.

Formatos de cadeias de caracteres

Estas propriedades aplicam-se à formatação de cadeias de caracteres:

- São permitidos comentários através de sintaxe XML padrão.

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

- São permitidos espaço em branco à esquerda e à direita para facilitar a leitura, mas são removidos do valor de parâmetro.
- As novas linhas dentro de um valor são convertidas em espaços.
- É permitido um cabeçalho XML com o formato `<? ?>`, mas o telefone ignora-o.
- Para introduzir caracteres especiais, utilize escapes de caracteres XML básicos, conforme indicado na tabela a seguir.

Carácter especial	Sequência de escape XML
& (e comercial)	&
< (menor que)	<
> (maior que)	>
’ (apóstrofo)	'
” (aspas)	"

No exemplo que se segue, os escapes são inseridos para representar os símbolos "maior que" e "menor que" necessários numa regra de plano de marcação. Este exemplo define um plano de marcação para linha de informações que define o parâmetro <Dial_Plan_1_> (**Início de sessão do administrador** > **Avançado** > **Voz** > **Ext (n)**) para igual a (S0 <:18005551212>).

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

- Os escapes de caracteres numéricos, com valores decimais e hexadecimais (s.a. `(` e `.`) são traduzidos.
- O firmware do telefone suporta apenas caracteres ASCII.

Compressão e encriptação de perfil aberto (XML)

O perfil Abrir configuração pode ser comprimido para reduzir a carga de rede no servidor de aprovisionamento. O perfil também pode ser encriptado para proteger informações confidenciais. A compressão não é obrigatória, mas deve ser feita antes da encriptação.

Tópicos relacionados

Formatos de perfil de configuração, na página 13

Compressão de perfil aberto

O método de compressão suportado é o algoritmo deflate gzip (RFC1951). O utilitário gzip e a biblioteca de compressão que implementa o mesmo algoritmo (zlib) estão disponíveis em sites da Internet.

Para identificar a compressão, o telefone espera que o ficheiro comprimido contenha um cabeçalho compatível com gzip. A invocação do utilitário gzip no perfil aberto original gera o cabeçalho. O telefone verifica o cabeçalho do ficheiro transferido para determinar o formato do ficheiro.

Por exemplo, se `profile.xml` for um perfil válido, o ficheiro `profile.xml.gz` também é aceite. Qualquer um dos seguintes comandos pode gerar este tipo de perfil:

- `> gzip profile.xml`

  Substitui o ficheiro original com ficheiro comprimido.

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

  Deixa o ficheiro original, produz novo ficheiro comprimido.

Na secção Comprimir um perfil aberto com Gzip, na página 63 é fornecido um tutorial sobre compressão.

Tópicos relacionados

Comprimir um perfil aberto com Gzip, na página 63

Encriptação de perfil aberto

É possível utilizar encriptação de chave simétrica para encriptar um perfil de configuração aberto, esteja o ficheiro comprimido ou não. A compressão, se aplicada, tem de ser aplicada antes da encriptação.

O servidor de aprovisionamento utiliza HTTPS para lidar com o aprovisionamento inicial do telefone após a implementação. A pré-encriptação dos perfis de configuração offline permite a utilização de HTTP para a ressincronização de perfis subsequentemente. Isto reduz a carga no servidor HTTPS em implementações em larga escala.

O telefone suporta dois métodos de encriptação para ficheiros de configuração:

- Encriptação AES-256-CBC
- Encriptação de conteúdo HTTP baseada em RFC 8188 com cifragem AES-128-GCM

A chave ou o IKM (Input Keying Material) deve ser pré-aprovisionado para a unidade previamente. É possível inicializar a chave secreta em segurança com HTTPS.

O nome do ficheiro de configuração não exige um formato específico, mas um nome de ficheiro que termine com a extensão `.cfg` indica normalmente um perfil de configuração.

Encriptação AES-256-CBC

O telefone suporta encriptação AES-256-CBC para os ficheiros de configuração.

A ferramenta de encriptação OpenSSL, disponível para transferência em vários sites de Internet, pode executar a encriptação. O suporte para encriptação AES de 256 bits pode exigir recompilação da ferramenta para ativar o código AES. O firmware foi testado em relação à versão openssl-0.9.7c.

Encriptar um perfil com OpenSSL, na página 63 oferece um tutorial sobre encriptação.

Para um arquivo encriptado, o perfil espera que o ficheiro tenha o mesmo formato que o gerado pelo seguinte 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
```

Uma letra -k minúscula precede a chave secreta, que pode ser qualquer frase de texto sem formatação, e que é utilizada para gerar um salt aleatório de 64 bits. Com o segredo especificado pelo argumento -k, a ferramenta de encriptação deriva um vetor inicial aleatório de 128 bits e a chave de encriptação de 256 bits real.

Quando esta forma de encriptação é utilizada num perfil de configuração, o telefone deve ser informado do valor da chave secreta para desencriptar o ficheiro. Este valor é especificado como qualificador no URL do perfil. A sintaxe é a seguinte, com um URL explícito:

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

Este valor é programado utilizando um dos parâmetros Profile_Rule.

Tópicos relacionados

Encriptar um perfil com OpenSSL, na página 63

Expansão via macro

Vários parâmetros de aprovisionamento passam por expansão via macro internamente antes de serem avaliados. Esta etapa de pré-avaliação oferece maior flexibilidade para controlar as atividades de atualização e ressincronização do telefone.

Estes grupos de parâmetro passam por expansão via macro antes da avaliação:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

Sob certas condições, alguns parâmetros genéricos (GPP_*) também passam por expansão via macro, conforme explicitamente indicado em Argumentos de ressincronização opcional, na página 23.

Durante a expansão via macro, o conteúdo das variáveis nomeadas substituem expressões da forma $NAME e $(NAME). Estas variáveis incluem parâmetros genéricos, vários identificadores de produto, determinadas durações de eventos e valores de estados de aprovisionamento. Para obter uma lista completa, consulte Variáveis de expansão via macro, na página 74.

No exemplo a seguir, a expressão $(MAU) é utilizada para introduzir o endereço MAC 000E08012345.

O administrador introduz: **`$(MAU)config.cfg`**

A expansão via macro resultante para um dispositivo com endereço MAC 000E08012345 é: `000E08012345config.cfg`

Se um nome de macro não for reconhecido, permanece sem expansão. Por exemplo, o nome STRANGE não é reconhecido como um nome de macro válido, enquanto MAU é reconhecido como um nome de macro válido.

O administrador introduz: **`$STRANGE$MAU.cfg`**

A expansão via macro resultante para um dispositivo com endereço MAC 000E08012345 é: `$STRANGE000E08012345.cfg`

A expansão via macro não é aplicada recursivamente. Por exemplo, $$MAU" expande para $MAU" (o $$ é expandido) e não resulta no endereço MAC.

O conteúdo dos parâmetros específicos, GPP_SA a GPP_SD, é mapeado para as expressões macro $SA a $SD. Estes parâmetros só são expandidos via macro como o argumento das opções **--key** , **--uid** e **--pwd** num URL de ressincronização.

Expressões condicionais

Expressões condicionais podem acionar eventos de ressincronização e selecionar URLs alternados para operações de ressincronização e atualização.

As expressões condicionais consistem numa lista de comparações, separados pelo operador **and**. Todas as comparações devem ser satisfeitas para a condição ser verdadeira.

Cada comparação pode relacionar-se com um dos seguintes tipos de literais:

- Valores inteiros
- Números de versão do software ou hardware
- Cadeias de caracteres entre aspas

Números de versão

A versão de software formal dos telefones multiplataforma (MPP) utiliza este formato, em que BN= =número da compilação:

- Cisco IP Phone 6800 Series — `sip68xx.v1-v2-v3MPP-BN`

A cadeia de caracteres de comparação deve utilizar o mesmo formato. Caso contrário, dá-se um erro de análise de formato.

Na versão do software, v1-v2-v3-v4 pode especificar diferentes dígitos ou caracteres, mas deve começar com um dígito numérico. Ao comparar a versão do software, v1-v2-v3-v4 é comparado em sequência e os dígitos mais à esquerda têm precedência sobre os outros.

Se v[x] inclui apenas dígitos numéricos, os dígitos são comparados; se v[x] inclui dígitos numéricos + caracteres alfabéticos, primeiro são comparados os dígitos e depois os caracteres por ordem alfabética.

Exemplo de número de versão válido

sipyyyy.11-0-0MPP-BN

Em contrapartida: 11.0.0 é um formato inválido.

Comparação

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

É possível comparar cadeias de caracteres entre aspas para encontrar igualdade ou desigualdade. Também é possível comparar aritmeticamente números inteiros e números de versão. Os operadores de comparação podem ser expressos como símbolos ou como acrónimos. Os acrónimos são convenientes para exprimir a condição num perfil de formato aberto.

Operador	Sintaxe alternativa	Descrição	Aplicável a operandos inteiros e de versão	Aplicável a operandos de cadeias de caracteres entre aspas
=	eq	igual a	Sim	Sim
!=	ne	não igual a	Sim	Sim
<	lt	é menor que	Sim	Não
<=	le	é menor do que ou igual a	Sim	Não
>	gt	é maior do que	Sim	Não
>=	ge	é maior do que ou igual a	Sim	Não
E		e	Sim	Sim

É importante colocar as variáveis de macro entre aspas onde se espera uma cadeia de caracteres literal. Não o faça quando se espera um número ou número de versão.

Quando utilizadas no contexto dos parâmetros Profile_Rule* e Upgrade_Rule, as expressões condicionais devem ser colocadas dentro da sintaxe "(expr)?" como neste exemplo de regra de atualização. Lembre-se de que BN significa número da compilação.

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

Não utilize a sintaxe anterior com parênteses para configurar os parâmetros Resync_Trigger_*.

Sintaxe do URL

Utilize a sintaxe de URL padrão para especificar a forma de recuperar ficheiros de configuração e cargas de firmware nos parâmetros Profile_Rule* e Upgrade_Rule, respetivamente. A sintaxe é a seguinte:

[esquema://] [servidor [:porta]] caminho do ficheiro

Em que **esquema** é um dos seguintes valores:

- tftp
- http
- https

Se **esquema** for omitido, a predefinição é tftp. O servidor pode ser um nome de anfitrião reconhecido por DNS ou um endereço IP numérico. A porta é o número de porta de destino UDP ou TCP. O caminho do ficheiro deve começar com o diretório raiz (/); deve ser um caminho absoluto.

Se o **servidor** estiver ausente, é utilizado o servidor tftp especificado por DHCP (opção 66).

Nota Para regras de atualização é necessário especificar o servidor.

Se a **porta** estiver ausente, é utilizada a porta padrão para o esquema especificado. Tftp utiliza a porta UDP 69, http utiliza a porta TCP 80, https utiliza a porta TCP 443.

É necessário estar presente um caminho de ficheiro. Não tem necessariamente de referir um ficheiro estático, mas pode indicar conteúdo dinâmico obtido por CGI.

A expansão via macro aplica-se nos URLs. Seguem-se exemplos de URLs válidos:

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

Ao utilizar a opção 66 do DHCP, a sintaxe vazia não é suportada por regras de atualização. Só é aplicável para o perfil de regra*.

Encriptação de conteúdo HTTP com base em RFC 8188

O telefone suporta encriptação de conteúdo HTTP baseada em RFC 8188 com cifragem AES-128-GCM para ficheiros de configuração. Com este método de encriptação, qualquer entidade pode ler os cabeçalhos de mensagens HTTP. No entanto, só as entidades que conhecem o IKM (Input Keying Material) podem ler o payload. Quando o telefone está aprovisionado com o IKM, o telefone e o servidor de aprovisionamento podem trocar ficheiros de configuração de forma segura, permitindo que elementos de rede terceiros utilizem os cabeçalhos de mensagens para fins de análise e monitorização.

O parâmetro de configuração XML **IKM_HTTP_Encrypt_Content** mantém o IKM no telefone. Por razões de segurança, este parâmetro não está acessível na página Web de administração do telefone. Também não é visível no ficheiro de configuração do telefone, ao qual pode aceder a partir do endereço IP do telefone ou de relatórios de configuração do telefone enviados para o servidor de aprovisionamento.

Se pretender utilizar a encriptação com base em RFC 8188, certifique-se do seguinte:

- Aprovisione o telefone com o IKM, especificando o IKM com o parâmetro XML **IKM_HTTP_Encrypt_Content** no ficheiro de configuração que é enviado do servidor de aprovisionamento para o telefone.
- Se esta encriptação for aplicada aos ficheiros de configuração enviados do servidor de aprovisionamento para o telefone, certifique-se de que o cabeçalho HTTP *Content-Encoding* no ficheiro de configuração tem "aes128gcm".

  Na ausência deste cabeçalho, o método AES-256-CBC tem precedência. O telefone aplica a desencriptação AES-256-CBC se existir uma chave AES-256-CBC numa regra de perfil, independentemente do IKM.
- Se pretender que o telefone aplique esta encriptação aos relatórios de configuração que envia para o servidor de aprovisionamento, certifique-se de que não existe nenhuma chave AES-256-CBC especificada na regra de relatórios.

Argumentos de ressincronização opcional

Os URLs inseridos nos parâmetros Profile_Rule* podem ser precedidos de argumentos opcionais como **key**, **uid** e **pwd**, coletivamente entre parênteses retos.

tecla

A opção **--key** indica ao telefone que o ficheiro de configuração que recebe do servidor de aprovisionamento está encriptado com encriptação AES-256-CBC, a menos que o cabeçalho *Content-Encoding* no ficheiro indique encriptação "aes128gcm". A chave em si é especificada como cadeia após o termo **--key**. A chave pode estar, opcionalmente, entre aspas duplas ("). O telefone utiliza a chave para desencriptar o ficheiro de configuração.

Exemplos de utilização

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

Os argumentos opcionais agrupados são expandidos via macro. Os parâmetros específicos, GPP_SA até GPP_SD, são expandidos via macro para variáveis de macro, $SA a $SD, apenas quando são utilizados como argumentos de opção de chave. Consulte estes exemplos:

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

Nos perfis de formato aberto, o argumento para **--key** deve ser o mesmo que o argumento para a opção **-k** atribuída ao **openssl**.

uid e pwd

As opções **uid** e **pwd** opções podem ser utilizadas para especificar a autenticação com ID de utilizador e palavra-passe para o URL especificado. Os argumentos opcionais agrupados são expandidos via macro. Os parâmetros específicos, GPP_SA até GPP_SD, são expandidos via macro para variáveis de macro, $SA a $SD, apenas quando são utilizados como argumentos de opção de chave. Consulte estes exemplos:

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

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

seria expandido para:

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

Aplicar um perfil ao dispositivo de telefonia IP

Após criar um script de configuração XML, ele deve ser passado ao telefone para aplicação. Para aplicar a configuração, pode transferir o ficheiro de configuração para o telefone a partir de um servidor TFTP, HTTP ou HTTPS com um web browser, ou usando o utilitário de linha de comando cURL.

Transferir o ficheiro de configuração para o telefone a partir de um servidor TFTP

Efetue os seguintes procedimentos para transferir o ficheiro de configuração para uma aplicação de servidor TFTP no seu PC.

Procedure

Passo 1 Ligue o seu PC ao telefone LAN.

Passo 2 Execute uma aplicação de servidor TFTP no PC e certifique-se de que o ficheiro de configuração está disponível no diretório raiz TFTP.

Passo 3 Num web browser, introduza o endereço IP do telefone LAN, o endereço IP do computador, o nome do ficheiro e as credenciais de início de sessão. Utilize este formato:

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

Exemplo:

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

Transferir o ficheiro de configuração para o telefone com cURL

Efetue os seguintes procedimentos para transferir a configuração para o telefone com cURL. Esta ferramenta de linha de comando é utilizada para transferir dados com uma sintaxe de URL. Para transferir cURL, visite:

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

Nota Recomendamos que não utilize cURL para publicar a configuração no telefone, porque o nome de utilizador e palavra-passe podem ser capturados ao utilizar cURL.

Procedure

Passo 1 Ligue o PC à porta LAN do telefone.

Passo 2 Transfira o ficheiro de configuração para o telefone introduzindo o seguinte comando cURL:

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

Parâmetros de aprovisionamento

Esta secção descreve os parâmetros de aprovisionamento amplamente organizados de acordo com a função:

Existem os seguintes tipos de parâmetro de aprovisionamento:

- Genéricos
- Ativadores
- Acionadores
- Agendas configuráveis
- Regras de perfil
- Regra de atualização

Parâmetros genéricos

Os parâmetros genéricos GPP_* (**Início de sessão do administrador** > **Avançado** > **Voz** > **Aprovisionamento**) são utilizados como registos de cadeia de caracteres livre ao configurar o telefone para interagir com uma solução de servidor de aprovisionamento específico. Os parâmetros GPP_* estão vazios por predefinição. Podem ser configurados para conter valores diversos, incluindo os seguintes:

- Chaves de encriptação
- URLs
- Várias fases de informações de estado de aprovisionamento
- Modelos de pedido POST
- Mapas alias de nome do parâmetro
- Valores de cadeia de caracteres parciais, eventualmente combinados em valores de parâmetros completos.

Os parâmetros GPP_* estão disponíveis para expansão via macro dentro de outros parâmetros de aprovisionamento. Para este fim, os nomes de macro constituídos por uma única letra maiúscula (A a P) são suficientes para identificar o conteúdo de GPP_A a GPP_P. Além disso, os nomes de macro constituídos por duas letras maiúsculas SA a SD identificam GPP_SA a GPP_SD como um caso especial quando utilizados como argumentos das seguintes opções de URL:

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

Estes parâmetros podem ser utilizados como variáveis em regras de aprovisionamento e atualização. São referenciados acrescentando ao nome da variável um prefixo com um carácter '$', como por exemplo $GPP_A.

Utilizar parâmetros genéricos

Por exemplo, se GPP_A contiver a cadeia de caracteres ABC, e GPP_B contiver 123, a expressão AB expande via macro para ABC123.

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Selecione **Voz** > **Aprovisionamento**.

Passo 2 Desloque-se até à secção **Parâmetros genéricos**.

Passo 3 Introduza valores válidos nos campos GPP A até GPP P.

Passo 4 Clique em **Submeter todas as alterações**.

Ativadores

Os parâmetros Provision_Enable e Upgrade_Enable controlam todas as operações de atualização do firmware e ressincronização de perfil. Estes parâmetros controlam ressincronizações e atualizações independentemente uns dos outros. Estes parâmetros também controlam ressincronizações e comandos de atualização de URL emitidos pelo servidor Web da administração. Ambos estes parâmetros estão definidos para **Sim** por predefinição.

O parâmetro Resync_From_SIP controla os pedidos de operações de ressincronização. Um evento SIP NOTIFY é enviado do servidor proxy do provedor de serviços para o telefone. Se estiver ativado, o proxy pode pedir uma ressincronização. Para o fazer, o proxy envia uma mensagem SIP NOTIFY que contém o cabeçalho Event:resync para o dispositivo.

O dispositivo desafia o pedido com uma resposta 401 (autorização recusada para as credenciais utilizadas). O dispositivo espera um pedido autenticado subsequente antes de respeitar o pedido de ressincronização do proxy. Os cabeçalhos Event: reboot_now e Event: restart_now realizam reinícios a frio e a quente, respetivamente, que também são desafiados.

Os dois ativadores restantes são Resync_On_Reset e Resync_After_Upgrade_Attempt. Estes parâmetros determinam se o dispositivo executa uma operação de ressincronização depois de reinícios de software de ligação e após cada tentativa de atualização.

Quando é ativado o Resync_On_Reset, o dispositivo introduz um atraso aleatório que segue a sequência de inicialização antes de a reposição ser executada. O atraso é um tempo aleatório até ao valor especificado pelo Resync_Random_Delay (em segundos). Num conjunto de telefones que ligam ao mesmo tempo, este atraso espalha as horas de início dos pedidos de ressincronização de cada unidade. Esta funcionalidade pode ser útil numa implementação residencial grande, no caso de uma falha de energia regional.

Acionadores

O telefone permite ressincronizar com intervalos específicos ou num horário específico.

Ressincronizar com intervalos específicos

O telefone foi desenvolvido para ressincronizar periodicamente com o servidor de aprovisionamento. O intervalo de ressincronização é configurado em Resync_Periodic (segundos). Se este valor for deixado vazio, o dispositivo não ressincroniza periodicamente.

A ressincronização ocorre normalmente quando as linhas de voz estão inativas. Se uma linha de voz estiver ativa quando chegar a altura de ressincronizar, o telefone atrasa o procedimento de ressincronização até a linha ficar novamente inativa. Uma ressincronização alterar os valores de parâmetros de configuração.

Uma operação de ressincronização pode falhar porque o telefone não consegue recuperar um perfil do servidor, o ficheiro transferido está corrompido ou ocorreu um erro interno. O dispositivo tenta ressincronizar novamente após um período especificado em Resync_Error_Retry_Delay (segundos). Se Resync_Error_Retry_Delay estiver definido para 0, o dispositivo não tenta ressincronizar novamente após uma tentativa falhada de ressincronização.

Se uma atualização falhar, é executada uma nova tentativa após Upgrade_Error_Retry_Delay segundos.

Estão disponíveis dois parâmetros configuráveis para acionar condicionalmente uma ressincronização: Resync_Trigger_1 e Resync_Trigger_2. Cada parâmetro pode ser programado com uma expressão condicional que passa por expansão via macro. Quando o intervalo de ressincronização expira (tempo para a próxima ressincronização), os acionadores, se definidos, impedem a ressincronização, a menos que um ou mais acionadores sejam avaliados como verdadeiro.

A seguinte condição de exemplo aciona uma ressincronização. No exemplo, a última tentativa de atualização do telefone ocorreu há mais de 5 minutos (300 segundos) e decorreram pelo menos 10 minutos (600 segundos) desde a última tentativa de ressincronização.

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

Ressincronizar numa altura específica

O parâmetro Resync_At permite ao telefone ressincronizar num horário específico. Este parâmetro utiliza o formato de 24 horas (hhmm) para especificar o horário.

O parâmetro Resync_At_Random_Delay permite ao telefone ressincronizar num horário com atraso não especificado. Este parâmetro utiliza um formato de número inteiro positivo para especificar o horário.

Deve evitar-se inundar o servidor com pedidos de ressincronização de vários telefones configurados para ressincronizar ao mesmo tempo. Para o fazer, o telefone aciona a ressincronização até 10 minutos após o horário especificado.

Por exemplo, se a hora de ressincronização estiver definida para 1000 (10h00), o telefone aciona a ressincronização a qualquer momento entre as 10h00 e as 10h10.

Por predefinição, a funcionalidade está desativada. Se o parâmetro Resync_At for aprovisionado, o parâmetro Resync_Periodic é ignorado.

Agendas configuráveis

É possível configurar agendas para ressincronizações periódicas, bem como especificar os intervalos de repetição para ressincronização e falhas de atualização utilizando os seguintes parâmetros de aprovisionamento:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Cada parâmetro aceita um valor de atraso único (segundos). A nova sintaxe alargada permite uma lista separada por vírgulas de elementos de atraso consecutivos. O último elemento na sequência é implicitamente repetido para sempre.

Opcionalmente, pode usar um sinal de adição para especificar outro valor numérico que acrescenta um atraso extra aleatório.

Exemplo 1

Neste exemplo, o telefone ressincroniza periodicamente de 2 em 2 horas. Se ocorrer uma falha de ressincronização, o dispositivo efetua novas tentativas com os seguintes intervalos: 30 minutos, 1 hora, 2 horas, 4 horas. O dispositivo continua a tentar em intervalos de 4 horas até ressincronizar com êxito.

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

Exemplo 2

Neste exemplo, o dispositivo ressincroniza periodicamente de hora a hora (mais um atraso extra aleatório de até 10 minutos). No caso de uma falha de ressincronização, o dispositivo efetua novas tentativas com os seguintes intervalos: 30 minutos (mais até 5 minutos). 1 hora (mais até 10 minutos), 2 horas (mais até 15 minutos). O dispositivo continua a tentar em intervalos de 2 horas (mais até 15 minutos) até ressincronizar com êxito.

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

Exemplo 3

Neste exemplo, se uma tentativa de atualização remota falhar, o dispositivo efetua uma nova tentativa de atualização após 30 minutos, outra após mais uma hora e outra após mais duas horas. Se a atualização continuar a falhar, o dispositivo efetua novas tentativas de quatro em quatro ou de cinco em cinco horas até a atualização ser bem-sucedida.

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

Regras de perfil

O telefone fornece vários parâmetros de perfil de configuração remota (Profile_Rule*). Assim, cada operação de ressincronização pode recuperar vários ficheiros geridos por servidores diferentes.

No cenário mais simples, o dispositivo ressincroniza periodicamente com um único perfil num servidor central, que atualiza todos os parâmetros internos pertinentes. Em alternativa, o perfil pode ser dividido entre diferentes ficheiros. Um ficheiro é comum para todos os telefones numa implantação. É fornecido para cada conta um ficheiro exclusivo separado. É possível fornecer chaves de encriptação e informações de certificado ainda por outro perfil, armazenado num servidor separado.

Sempre que deva ser efetuada uma operação de ressincronização, o telefone avalia os quatro parâmetros Profile_Rule* sequencialmente:

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

Cada avaliação pode resultar numa recuperação do perfil de um servidor de aprovisionamento remoto, com uma possível atualização de alguns parâmetros internos. Se uma avaliação falhar, a sequência de ressincronização é interrompida e tentada novamente desde o início especificado pelo parâmetro Resync_Error_Retry_Delay (segundos). Se todas as avaliações forem bem-sucedidas, o dispositivo aguarda até que ao segundo especificado pelo parâmetro Resync_Periodic e, em seguida, executa outra ressincronização.

O conteúdo de cada parâmetro Profile_Rule* consiste num conjunto de alternativas. As alternativas são separadas pelo carácter | (linha). Cada alternativa consiste numa expressão condicional, uma expressão de atribuição, um URL de perfil e quaisquer opções de URL associadas. Todos estes componentes são opcionais dentro de cada alternativa. Seguem-se as combinações válidas e a ordem por que devem aparecer, se estiverem presentes:

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

Dentro de cada parâmetro Profile_Rule*, todas as alternativas exceto a última devem fornecer uma expressão condicional. Esta expressão é avaliada e processada da seguinte forma:

1. As condições são avaliadas da esquerda para a direita, até ser localizada uma avaliada como verdadeira (ou até ser encontrada uma alternativa sem expressão condicional).
2. Qualquer expressão de atribuição a acompanhar é avaliada, se estiver presente.
3. Se for especificado um URL como parte dessa alternativa, é feita uma tentativa de transferir o perfil localizado no URL especificado. O sistema tenta atualizar os parâmetros internos em conformidade.

Se todas as alternativas tiverem expressões condicionais e nenhuma for avaliada como verdadeira (ou se toda a regra de perfil estiver vazia), todo o parâmetro Profile_Rule* é ignorado. É avaliado o próximo parâmetro de regra de perfil na sequência.

Exemplo 1

Este exemplo ressincroniza incondicionalmente com o perfil no URL especificado e executa um pedido HTTP GET ao servidor de aprovisionamento remoto:

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

Exemplo 2

Neste exemplo, o dispositivo ressincroniza com dois URLs diferentes, dependendo do estado de registo da Linha 1. Em caso de registo perdido, o dispositivo executa um HTTP POST para um script CGI. O dispositivo envia o conteúdo da GPP_A expandida via macro, que pode fornecer informações adicionais sobre o estado do dispositivo:

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

Exemplo 3

Neste exemplo, o dispositivo ressincroniza com o mesmo servidor. O dispositivo fornece informações adicionais, se não estiver instalado um certificado na unidade (para unidades de legado pré-2.0):

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

Exemplo 4

Neste exemplo, a Linha 1 fica desativada até GPP_A ser definido como igual a Aprovisionado pelo primeiro URL. Posteriormente, ressincroniza com o segundo URL:

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

Exemplo 5

Neste exemplo, parte-se do princípio de que o perfil devolvido pelo servidor contém marcadores de elementos XML. Estes marcadores devem ser remapeados para nomes de parâmetros adequados pelo mapa de aliases armazenado em GPP_B:

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

Uma ressincronização normalmente é considerada sem êxito se um perfil pedido não for recebido do servidor. O parâmetro Resync_Fails_On_FNF pode substituir este comportamento predefinido. Se Resync_Fails_On_FNF estiver definido como Não, o dispositivo aceita uma resposta de ficheiro-não-encontrado do servidor como uma ressincronização bem-sucedida. A predefinição para Resync_Fails_On_FNF é Sim.

Regra de atualização

A regra de atualização é instruir o dispositivo para ativar para uma nova carga e onde obter a carga, se necessário. Se a carga já estiver no dispositivo, ele não irá tentar obter a carga. Assim, a validade da localização da carga não importa quando a carga pretendida estiver na partição inativa.

A Upgrade_Rule especifica uma carga de firmware que, se for diferente da carga atual, irá ser transferida e aplicada a menos que seja limitada por uma expressão condicional ou o Upgrade_Enable estiver definido para **Não**.

O telefone fornece um parâmetro de atualização remoto configurável, Upgrade_Rule. Este parâmetro aceita sintaxe semelhante aos parâmetros da regra de perfil. As opções de URL não são suportadas para atualizações, mas podem ser utilizadas expressões condicionais e expressões de atribuição. Se forem utilizadas expressões condicionais, o parâmetro pode ser preenchido com várias alternativas, separadas pelo carácter |. A sintaxe para cada alternativa é a seguinte:

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

No caso dos parâmetros Profile_Rule*, o parâmetro de Upgrade_Rule avalia cada alternativa até satisfazer uma expressão condicional até uma alternativa não ter nenhuma expressão condicional. A expressão de atribuição a acompanhar é avaliada, se for especificado. Em seguida, é feita uma tentativa de atualização para o URL especificado.

Se o Upgrade_Rule contiver um URL sem expressão condicional, o dispositivo atualiza para a imagem de firmware especificada pelo URL. Depois da expansão via macro e da avaliação da regra, o dispositivo não tenta novamente atualizar até a regra ser modificada ou a combinação eficaz do esquema + servidor + porta + caminho do ficheiro ser alterada.

Para fazer uma tentativa de atualização de firmware, o dispositivo desativa o áudio no início do procedimento e reinicializa no fim do procedimento. O dispositivo começa automaticamente uma atualização controlada pelo conteúdo do Upgrade_Rule apenas se todas as linhas de voz estiverem atualmente inativas.

Por exemplo,

- Para o Cisco IP 6800 Series:

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

  where BN==Build Number
  ```

Neste exemplo, o Upgrade_Rule atualiza o firmware para a imagem armazenada no URL indicado.

Eis outro exemplo para o Cisco IP Phone 6800 Series:

```
("$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
```

Este exemplo direciona a unidade para carregar uma de duas imagens, com base no conteúdo de um parâmetro genérico, GPP_F.

O dispositivo pode impor um limite para mudar para uma versão anterior relativamente ao número de revisão do firmware, que pode ser uma opção de personalização útil. Se um número de revisão do firmware válido for configurado no parâmetro Downgrade_Rev_Limit, o dispositivo rejeita tentativas de atualização para versões de firmware anteriores ao limite especificado.

Tipos de dados

Estes tipos de dados são utilizados com parâmetros de configuração de perfil:

- {a, b, c,...} — Escolha entre a, b, c...
- Bool — Valor booleano de "sim" ou "não".

- CadScript — Um miniscript que especifica os parâmetros de cadência de um sinal. Até 127 caracteres.

  Sintaxe: S_1[; S_2], em que:

  - S_i=D_i($on_{i,1}$/$off_{i,1}$[,$on_{i,2}$/$off_{i,2}$[,$on_{i,3}$/$off_{i,3}$[,$on_{i,4}$/$off_{i,4}$[,$on_{i,5}$/$off_{i,5}$[,$on_{i,6}$/$off_{i,6}$]]]]]) e é conhecido por uma secção.
  - $on_{i,j}$ e $off_{i,j}$ are são a duração on/off em segundos de um *segmento*. i = 1 ou 2, e j = 1 a 6.
  - D_i é a duração total da secção em segundos.

  Todas as durações podem ter até três casas decimais para fornecer resolução 1 ms. O carácter universal "*" significa duração infinita. Os segmentos dentro de uma secção são reproduzidos por ordem e repetidos até ser reproduzida a duração total.

  Exemplo 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
```

  Exemplo 2 — Toque distinto (curto, curto, curto, longo):

```
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 — sintaxe de scripts utilizada para especificar os planos de marcação da Linha 1 e Linha 2.
- Float<n> — Um ponto de valor flutuante com até n casas decimais.
- FQDN — Nome de domínio completamente qualificado. Pode conter até 63 caracteres. Seguem-se alguns exemplos:
  - sip.Cisco.com:5060 ou 109.12.14.12:12345
  - sip.Cisco.com ou 109.12.14.12
- FreqScript — Um miniscript que especifica a os parâmetros de frequência e nível de um tom. Contém até 127 caracteres.

  Sintaxe: F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]], em que:

  - F_1– F_6 são a frequência em Hz (apenas números inteiros sem sinal).

- L_1– L_6 são níveis correspondentes em dBm (até uma casa decimal).

São permitidos, mas não se recomendam, espaços em branco antes e depois da vírgula.

Exemplo 1 — Tom de chamada em espera:

```
440@-10

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

Exemplo 2 — Tom de marcação:

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

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

- IP — Endereço IPv4 válido na forma de x.x.x. x, em que x está entre 0 e 255. Exemplo: 10.1.2.100.
- ID de utilizador — ID de utilizador conforme aparece num URL; até 63 caracteres.
- Telefone — uma sequência de número de telefone, como 14081234567, *69, *72, 345678; ou um URL genérico, como 1234@10.10.10.100:5068 ou jsmith@Cisco.com. A cadeia de caracteres pode conter até 39 caracteres.
- PhTmplt — um modelo de número de telefone. Cada modelo pode conter um ou mais padrões separados por vírgulas (,). Um espaço em branco no início de cada padrão é ignorado. “?” e “*” representam caracteres universais. Para representar literalmente, utilize xx %. Por exemplo, %2a representa *. O modelo pode conter até 39 caracteres. Exemplos: “1408*, 1510*”, “1408123????, 555?1.”.
- Porta — número da porta TCP/UDP (0-65535). Pode ser especificado em formato decimal ou hexadecimal.
- ProvisioningRuleSyntax — sintaxe de para scripts utilizada para definir as regras de atualização de firmware e ressincronização de configuração.
- PwrLevel — nível de energia expresso em dBm com uma casa decimal, como –13.5 ou 1.5 (dBm).
- RscTmplt — um modelo de código de estado de resposta SIP, como “404, 5*”, “61?”, “407, 408, 487, 481”. Pode conter até 39 caracteres.
- Sig<n> — valor n-bit com sinal. Pode ser especificado em formato decimal ou hexadecimal. Os valores negativos devem ser precedidos de um sinal “-”. Um sinal + antes de valores positivos é opcional.
- Códigos de asterisco — Código de ativação para um serviço complementar, como *69. O código pode conter até 7 caracteres.
- Str<n> — uma cadeia de caracteres genérica que tem até n caracteres não reservados.
- Time<n> — duração em segundos, com até n casas decimais. As casas decimais extra especificadas são ignoradas.
- ToneScript — um miniscript que especifica os parâmetros de frequência, nível e cadência de um sinal de chamada em curso. O script pode conter até 127 caracteres.

  Sintaxe: FreqScript;Z_1[;Z_2].

A secção Z_1 é semelhante à secção S_1 num CadScript, mas cada segmento on/off é seguido de um parâmetro de componentes de frequência: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$, em que:

- $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
- $1 < n_k < 6$ especifica os componentes de frequência no FreqScript que são utilizados nesse segmento.

Se for utilizado mais de um componente de frequência num segmento, os componentes são somados.

Exemplo 1 — Tom de marcação:

```
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
```

Exemplo 2 — Toque intermitente:

```
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 > — Valor n-bit sem sinal, em que n = 8, 16 ou 32. Pode ser especificado em formato decimal ou hexadecimal, como 12 ou 0x18, desde que o valor caiba em n bits.

Nota Tenha sempre em consideração:

- <Par Name> representa um nome de parâmetro de configuração. Num perfil, o marcador correspondente é formado substituindo o espaço por um sublinhado "_", como **Par_Name**.
- Um campo de valor predefinido vazio implica uma cadeia de caracteres vazia < “” >.
- O telefone continua a utilizar os últimos valores configurados para marcadores que não estão presentes num determinado perfil.
- Os modelos são comparados na ordem apresentada. É selecionada a primeira correspondência, *não a mais próxima*. O nome do parâmetro deve corresponder exatamente.
- Se for fornecida mais de uma definição de um parâmetro num perfil, as últimas dessas definições no ficheiro é a que entra em vigor no telefone.
- Uma especificação de parâmetros com um valor de parâmetros vazio força o parâmetro a regressar ao valor predefinido. Para especificar uma cadeia de caracteres vazia, utilize a cadeia de caracteres vazia "" como o valor do parâmetro.

Atualizações de perfil e atualizações de firmware

O telefone suporta atualizações remotas seguras de firmware e aprovisionamento (configuração). Um telefone não aprovisionado pode receber um perfil encriptado direcionado para esse dispositivo. O telefone não exige uma chave explícita devido a um mecanismo de primeiro aprovisionamento seguro que utiliza a funcionalidade SSL.

Não é necessária intervenção do utilizador para iniciar ou concluir uma atualização de perfil ou de firmware, ou se forem necessárias atualizações intermédias para atingir um estado de atualização futuro a partir de uma versão antiga. Só é feita uma tentativa de ressincronização de perfil quando o telefone está inativo, porque uma ressincronização pode acionar uma reinicialização do software e desligar uma chamada.

Os parâmetros genéricos gerem o processo de aprovisionamento. Cada telefone pode ser configurado para entrar periodicamente em contacto com um servidor de aprovisionamento normal (NPS). A comunicação com o NPS não exige a utilização de um protocolo seguro, porque o perfil atualizado é encriptado por uma chave secreta partilhada. O NPS pode ser um servidor TFTP, HTTP ou HTTPS padrão com certificados de cliente.

O administrador pode atualizar, reinicializar, reiniciar ou ressincronizar telefones utilizando a interface de utilizador do telefone da web. O administrador também pode realizar estas tarefas com uma mensagem de notificação SIP.

Os perfis de configuração são gerados com as ferramentas open-source comuns que integram com os sistemas de aprovisionamento do provedor de serviços.

Tópicos relacionados

Permitir e configurar atualizações de perfil, na página 35

Permitir e configurar atualizações de perfil

Podem ser permitidas atualizações de perfil em intervalos especificados. Os perfis atualizados são enviados de um servidor para o telefone através de TFTP, HTTP ou HTTPS.

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Selecione **Voz** > **Aprovisionamento**.

Passo 2 Na secção **Perfil de configuração**, escolha **Sim** na caixa de lista pendente **Ativar provisão**.

Passo 3 Introduza os parâmetros.

Passo 4 Clique em **Submeter todas as alterações**.

Tópicos relacionados

Atualizações de perfil e atualizações de firmware, na página 35

Permitir e configurar atualizações de firmware

Podem ser permitidas atualizações de firmware em intervalos especificados. O firmware atualizado é enviado de um servidor para o telefone através de TFTP ou HTTP. A segurança é menos problemática com uma atualização de firmware, porque o firmware não contém informações pessoais.

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Selecione **Voz** > **Aprovisionamento**.

Passo 2 Na secção **Atualização de firmware**, escolha **Sim** a partir da caixa de lista pendente **Ativar atualização**.

Passo 3 Introduza os parâmetros.

Passo 4 Clique em **Submeter todas as alterações**.

Atualização de firmware por TFTP, HTTP ou HTTPS

O telefone suportar a atualização única de uma só imagem por TFTP, HTTP ou HTTPS.

Nota As mudanças para as versões anteriores podem não estar disponíveis para todos os dispositivos. Para obter mais informações, consulte as notas de versão para o seu telefone e versão de firmware.

Before you begin

O ficheiro de carga de firmware deve ser transferido para um servidor acessível.

Procedure

Passo 1 Mude o nome da imagem da seguinte forma:

`cp-x8xx-sip.aa-b-cMPP.cop` para **`cp-x8xx-sip.aa-b-cMPP.tar.gz`**

onde

`x8xx` é a série do telefone, como 6841.

`aa-b-c` é o número de versão, como 10-4-1

Passo 2 Utilize o comando **`tar - xzvf`** para expandir o ficheiro tar.

Passo 3 Copie a pasta para um diretório de transferência TFTP, HTTP, ou HTTPS.

Passo 4 Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Passo 5 Selecione **Voz** > **Aprovisionamento**.

Passo 6 Localize o nome do ficheiro de carga que termina em **.loads** e anexe-o ao URL válido.

Passo 7 Clique em **Submeter todas as alterações**.

Atualizar firmware com um comando de browser

Um comando de atualização introduzido na barra de endereços do browser pode ser utilizado para atualizar o firmware do telefone. O telefone atualiza apenas quando está inativo. É feita uma tentativa automática de atualização após chamada ser concluída.

Procedure

Para atualizar o telefone com um URL num web browser, introduza este comando:

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

CAPÍTULO 3

Pré-aprovisionamento interno e servidores de aprovisionamento

Pré-aprovisionamentointernoeservidoresdeaprovisionamento

O provedor de serviços pré-aprovisiona os telefones, exceto as unidades RC, com um perfil. O perfil de pré-aprovisionamento pode conter um conjunto limitado de parâmetros que ressincroniza o telefone. O perfil também pode conter um conjunto completo de parâmetros fornecidos pelo servidor remoto. Por predefinição, o telefone ressincroniza ao ligar e em intervalos configurados no perfil. Quando o utilizador liga o telefone nas instalações do cliente, o dispositivo transfere o perfil atualizado e quaisquer atualizações de firmware.

Este processo de pré-aprovisionamento, implementação e aprovisionamento remoto pode ser efetuado de várias formas.

Preparação do servidor e ferramentas de software

Os exemplos neste capítulo exigem a disponibilidade de um ou mais servidores. Estes servidores podem ser instalados e executados num PC local:

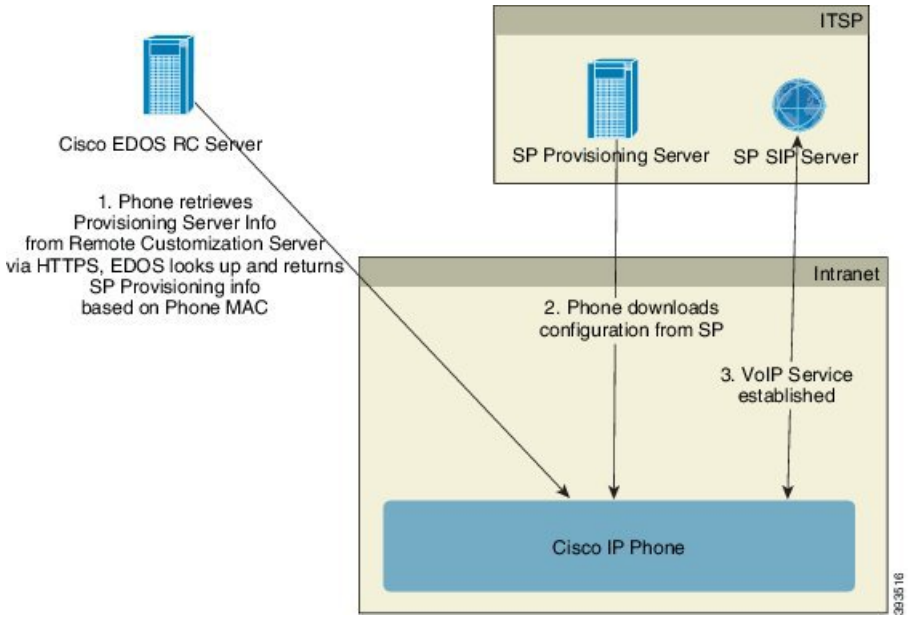
- TFTP (porta UDP 69)
- syslog (porta UDP 514)
- HTTP (porta TCP 80)
- HTTPS (porta TCP 443).

Para resolver problemas de configuração do servidor, é útil instalar os clientes de cada tipo de servidor numa máquina de servidor separada. Esta prática estabelece o funcionamento adequado do servidor, independentemente da interação com os telefones.

Também recomendamos que instale as seguintes ferramentas de software:

- Para gerar perfis de configuração, instale o utilitário de compressão open source gzip.
- Para encriptação de perfil e operações de HTTPS, instale o pacote de software open source OpenSSL.
- Para testar a geração de perfis dinâmicos e aprovisionamento remoto num passo usando HTTPS, recomendamos uma linguagem de script com suporte para scripts CGI. As ferramentas open source de linguagem Perl são exemplo de uma dessas linguagens de script.
- Para verificar as trocas seguras entre os servidores de aprovisionamento e os telefones, instale um sniffer de pacote de Ethernet (como o Ethereal/Wireshark com transferência gratuita). Capture um rastreamento de pacotes Ethernet da interação entre o telefone e o servidor de aprovisionamento. Para o fazer, execute o sniffer de pacotes num PC ligado a um comutador com espelhamento de porta ativado. Para transações HTTPS, pode usar o utilitário ssldump.

Distribuição de personalização remota (RC)



Todos os telefones contactam o servidor de personalização remota EDOS da Cisco CR até serem inicialmente aprovisionados.

Num modelo de distribuição de personalização remota, um cliente adquire um telefone que já foi associado a um Provedor de serviços específico no servidor de personalização remota EDOS da Cisco. O provedor de serviços de telefonia por Internet (ITSP) configura e mantém um servidor de aprovisionamento, e regista as respetivas informações do servidor de aprovisionamento com o servidor de personalização remota EDOS da Cisco.

Quando o telefone estiver ligado com uma ligação à Internet, o estado de personalização para o telefone não aprovisionado é **Aberto**. O telefone consulta primeiro o servidor DHCP local para obter informações do servidor de aprovisionamento e define o estado de personalização do telefone. Se a consulta DHCP for bem-sucedida, o estado de personalização é definido como **Abortado** e não existe tentativa de personalização remota porque o DHCP fornece as informações do servidor de aprovisionamento necessárias.

Quando um telefone estabelece ligação a uma rede pela primeira vez ou após uma reposição de fábrica, se não existir uma configuração de opções de DHCP, o telefone contacta um servidor de ativação de dispositivos

para aprovisionamento sem assistência. Novos telefones utilizarão “activate.cisco.com” em vez de “webapps.cisco.com” para aprovisionamento. Os telefones com versão de firmware anterior a 11.2 (1) continuarão a utilizar webapps.cisco.com. A Cisco recomenda que autorize ambos os nomes de domínio na sua firewall.

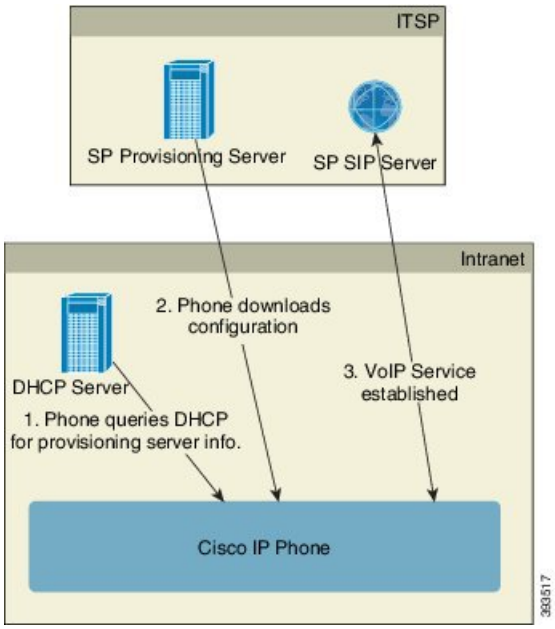
Se o servidor DHCP não fornecer informações do servidor de aprovisionamento, o telefone consulta o servidor de personalização remota EDOS da Cisco e fornece o respetivo modelo e endereço MAC, e o estado de personalização é definido como **Pendente**. O servidor EDOS da Cisco responde com as informações do servidor de aprovisionamento do provedor de serviços associado, incluindo o URL do servidor de aprovisionamento, e o estado de personalização do telefone é definido como **Personalização pendente**. O telefone executa então um comando de ressincronização de URL para recuperar a configuração do Provedor de serviços e, se for bem-sucedido, o estado de personalização é definido como **Adquirido**.

Se o servidor de personalização remota EDOS da Cisco não tiver um provedor de serviços associado ao telefone, o estado de personalização do telefone é definido como **Indisponível**. O telefone pode ser configurado manualmente ou pode ser adicionada ao servidor de personalização remota EDOS da Cisco uma associação ao provedor de serviços do telefone.

Se um telefone é aprovisionado através de LCD do utilitário de configuração Web, antes do estado de personalização passar a **Adquirido**, o estado de personalização é definido como **Abortado** e o servidor de personalização remota EDOS da Cisco não é consultado, a menos que sejam repostas as definições de fábrica do telefone.

Depois de o telefone ter sido aprovisionado, o servidor de personalização remota EDOS da Cisco não é utilizado a menos que sejam repostas as definições de fábrica do telefone.

Pré-aprovisionamento interno do dispositivo



Com a predefinição de fábrica da Cisco, o telefone tenta automaticamente ressincronizar com um perfil num servidor TFTP. Um servidor DHCP gerido numa LAN fornece ao dispositivo as informações sobre o perfil e o servidor TFTP configurado para pré-aprovisionamento. O provedor de serviços liga cada novo telefone à LAN. O telefone ressincroniza automaticamente com o servidor TFTP local e inicializa o respetivo estado

interno em preparação para implementação. Este perfil de pré-aprovisionamento normalmente inclui o URL de um servidor de aprovisionamento remoto. O servidor de aprovisionamento mantém o dispositivo atualizado após a implementação e ligação do dispositivo à rede do cliente.

O código de barras do dispositivo pré-aprovisionado pode ser lido para registar o respetivo endereço MAC ou número de série antes de enviar o telefone ao cliente. Estas informações podem ser utilizadas para criar o perfil com o qual o telefone ressincroniza.

Ao receber o telefone, o cliente liga-o à ligação de banda larga. Ao ligar, o telefone entra em contacto com o servidor de aprovisionamento através do URL configurado por pré-aprovisionamento. O telefone pode assim ressincronizar e atualizar o perfil e o firmware, conforme necessário.

Tópicos relacionados

Distribuição a retalho, na página 5
Aprovisionamento TFTP, na página 42

Configuração do servidor de aprovisionamento

Esta secção descreve os requisitos de configuração para o aprovisionamento de um telefone utilizando vários servidores e diferentes cenários. Para os efeitos deste documento e de teste, os servidores de aprovisionamento são instalados e executados num PC local. Além disso, as ferramentas de software geralmente disponíveis são úteis para o aprovisionamento dos telefones.

Aprovisionamento TFTP

Os telefones oferecem suporte TFTP tanto para ressincronizações de aprovisionamento como para operações de atualização de firmware. Quando os dispositivos são instalados remotamente, recomenda-se HTTPS, mas também é possível utilizar HTTP e TFTP. Neste caso é necessário o aprovisionamento de encriptação de ficheiros para mais segurança, pois isso oferece maior fiabilidade, dados os mecanismos de proteção de NAT e router. TFTP é útil para o pré-aprovisionamento interno de um grande número de dispositivos não aprovisionados.

O telefone é capaz de obter um endereço IP de um servidor TFTP diretamente do servidor DHCP através da opção DHCP 66. Se estiver configurado um Profile_Rule com o caminho do ficheiro desse servidor TFTP, o dispositivo transfere o perfil do servidor TFTP. A transferência ocorre quando o dispositivo está ligado a uma LAN e ligado.

O Profile_Rule fornecido com a configuração predefinida de fábrica é *&PN*. cfg, em que *&PN* representa o nome do modelo de telefone.

Por exemplo, para uma CP-6841-3PCC, o nome do ficheiro é CP-6841-3PCC.cfg.

Para um dispositivo com o perfil predefinido de fábrica, ao ligar, o dispositivo ressincroniza com este ficheiro no servidor TFTP local que a opção DHCP 66 especifica. O caminho do ficheiro está relacionado com o diretório raiz virtual do servidor TFTP.

Tópicos relacionados

Pré-aprovisionamento interno do dispositivo, na página 41

NAT e controlo de ponto final remoto

O telefone é compatível com tradução de endereço de rede (NAT) para aceder à Internet através de um router. Para maior segurança, o router pode tentar bloquear pacotes recebidos não autorizados implementando NAT

simétrica, uma estratégia de filtragem de pacotes que limita drasticamente os pacotes que têm permissão para entrar na rede protegida a partir da Internet. Por este motivo, não se recomenda o aprovisionamento remoto com TFTP.

VoIP só pode coexistir com NAT quando é fornecida alguma forma de NAT transversal. Configure a travessia simples do UDP na NAT (STUN). Esta opção exige que o utilizador tenha:

- Um endereço IP dinâmico externo (público) a partir do seu serviço
- Um computador que execute o software de servidor STUN
- Um dispositivo de rede com um mecanismo NAT assimétrico

Aprovisionamento HTTP

O telefone comporta-se como um browser que pede páginas da Web a um site remoto de Internet. Este comportamento oferece um meio fiável de chegar ao servidor de aprovisionamento, mesmo quando um router cliente implementa NAT simétrica ou outros mecanismos de proteção. HTTP e HTTPS funcionam de forma mais fiável que TFTP em implementações remotas, especialmente quando as unidades implementadas são ligadas atrás de firewalls residenciais ou routers com capacidade para NAT. HTTP e HTTPs são utilizados indistintamente nas seguintes descrições de tipo de pedido.

O aprovisionamento básico com base em HTTP depende do método HTTP GET para recuperar perfis de configuração. Normalmente é criado um ficheiro de configuração para cada telefone implementado, e estes ficheiros são armazenados num diretório de servidor HTTP. Quando o servidor recebe o pedido GET, limita-se a devolver o ficheiro especificado no cabeçalho do pedido GET.

Em vez de um perfil estático, o perfil de configuração pode ser gerado dinamicamente consultando uma base de dados de cliente e produzindo o perfil rapidamente.

Quando o telefone pede uma ressincronização, pode utilizar o método HTTP POST para pedir os dados de configuração da ressincronização. O dispositivo pode ser configurado para transmitir determinadas informações de estado e identificação ao servidor dentro do corpo do pedido HTTP POST. O servidor utiliza estas informações para gerar um perfil de configuração de resposta pretendida, ou para armazenar as informações de estado para posterior análise e rastreamento.

Como parte dos pedidos GET e POST, o telefone inclui automaticamente informações básicas de identificação no campo de Utilizador-Agente do cabeçalho do pedido. Estas informações transmitem o fabricante, o nome do produto, a versão de firmware atual e o número de série do dispositivo.

O exemplo que se segue é o campo de pedido Utilizador-Agente de um CP-6841-3PCC:

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

Quando o telefone estiver configurado para ressincronizar com um perfil de configuração com HTTP, é recomendável utilizar HTTPS ou encriptar o perfil para proteger informações confidenciais. Os perfis encriptados que o telefone transfere através de HTTP evitam o perigo de exposição de informações confidenciais contidas no perfil de configuração. Este modo de ressincronização produz uma carga de computação inferior no servidor de aprovisionamento em comparação com a utilização de HTTPS.

O telefone pode desencriptar perfis com um dos seguintes métodos de encriptação:

- Encriptação AES-256-CBC
- Encriptação baseada em RFC-8188 com cifragem AES-128-GCM

Nota Os telefones suportam HTTP versão 1.0, HTTP versão 1.1 e Codificação de segmentos quando o protocolo de transporte negociado é HTTP versão 1.1.

Tratamento do código de estado HTTP em ressincronização e atualização

O telefone suporta resposta HTTP para aprovisionamento remoto (ressincronização). O comportamento atual do telefone é categorizado de três formas:

- A — Sucesso, em que os valores "Ressincronização periódica" e "Ressincronizar com atraso aleatório" determinam os pedidos subsequentes.
- B — Falha em caso de Ficheiro não encontrado ou perfil corrompido. O valor "Atraso de repetição após erro na ressincronização" determina os pedidos subsequentes.
- C — Outra falha quando um endereço IP ou URL incorretos provocam um erro de ligação. O valor "Atraso de repetição após erro na ressincronização" determina os pedidos subsequentes.

Tabela 2: Comportamento do telefone para respostas HTTP

Código de estado HTTP	Descrição	Comportamento do telefone
301 Movido permanentemente	Este pedido e pedidos futuros devem ser direcionados para uma nova localização.	Repetir imediatamente o pedido com nova localização.
302 Encontrado	Conhecido como Movido temporariamente.	Repetir imediatamente o pedido com nova localização.
3xx	Outras respostas 3xx não processadas.	C
400 Pedido incorreto	O pedido não pode ser concluído devido a sintaxe incorreta.	C
401 Não autorizado	Desafio de autenticação de acesso condensada ou básica.	Repetir imediatamente o pedido com credenciais de autenticação. Máximo de 2 novas tentativas. Após a falha, o comportamento do telefone é C.
403 Proibido	Servidor recusa-se a responder.	C
404 Não encontrado	Recurso pedido não encontrado. São permitidos pedidos subsequentes por parte do cliente.	B
407 Autenticação de proxy necessária	Desafio de autenticação de acesso condensada ou básica.	Repetir imediatamente o pedido com credenciais de autenticação. Máximo de duas novas tentativas. Após a falha, o comportamento do telefone é C.

Código de estado HTTP	Descrição	Comportamento do telefone
4xx	Outros códigos de estado de erro do cliente não são processados.	C
500 Erro interno de servidor	Mensagem de erro genérica.	O comportamento do telefone é C.
501 Não implementado	O servidor não reconhece o método de pedido ou não tem capacidade para concluir o pedido.	O comportamento do telefone é C.
502 Gateway incorreto	O servidor funciona como um gateway ou proxy e recebe uma resposta inválida do servidor a montante.	O comportamento do telefone é C.
503 Serviço indisponível	O servidor está atualmente indisponível (sobrecarregado ou para desativado para manutenção). Trata-se de um estado temporário.	O comportamento do telefone é C.
504 Tempo limite para gateway	O servidor funciona como um gateway ou proxy e não recebe uma resposta do servidor a montante dentro do tempo especificado.	C
5xx	Outro erro de servidor	C

Aprovisionamento HTTPS

O telefone suporta HTTPS para aprovisionamento para aumentar a segurança na gestão de unidades implementadas remotamente. Cada telefone tem um certificado de cliente SLL exclusivo (e chave privada associada), além de um certificado de raiz do servidor de autoridade de certificação Sipura. Este último permite ao telefone reconhecer servidores de aprovisionamento autorizados e rejeitar servidores não autorizados. Por outro lado, o certificado de cliente permite ao servidor de aprovisionamento identificar o dispositivo individual que emite o pedido.

Para um provedor de serviços gerir a implementação com HTTPS, é necessário gerar um certificado de servidor para cada servidor de aprovisionamento com o qual um telefone ressincroniza com HTTPS. O certificado do servidor deve ser assinado pela chave de raiz de certificado de autoridade do servidor Cisco, cujo certificado está presente em todas as unidades implementadas. Para obter um certificado de servidor assinado, o provedor de serviços deve encaminhar um pedido de assinatura de certificado à Cisco, que assina e devolve o certificado do servidor para instalação no servidor de aprovisionamento.

O certificado do servidor de aprovisionamento deve conter o campo de nome comum (CN) e o FQDN do anfitrião que executa o servidor no contexto. Opcionalmente, pode conter informações após o FQDN do anfitrião, separadas por um carácter de barra (/). Os exemplos que se seguem são de entradas CN aceites como válidas pelo telefone:

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

Além de verificar o certificado do servidor, o telefone testa o endereço IP do servidor em relação a uma pesquisa DNS do nome do servidor especificado no certificado do servidor.

Obter um certificado de servidor assinado

O utilitário OpenSSL pode gerar um pedido de assinatura de certificado. O exemplo a seguir mostra o comando **openssl** que produz um par de chaves pública/privada de 1024 bits RSA e um pedido de assinatura de certificado:

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

Este comando gera a chave privada do servidor no **privkey.pem** e um pedido de assinatura de certificado correspondente no **provserver.csr**. O provedor de serviços mantém secreto o **privkey.pem** e envia o **provserver.csr** à Cisco para assinatura. Ao receber o ficheiro **provserver.csr**, a Cisco gera o **provserver.crt**, o certificado do servidor assinado.

Procedure

Passo 1 Navegue até https://software.cisco.com/software/edos/home e registe-se com as suas credenciais CCO.

Nota Quando um telefone estabelece ligação a uma rede pela primeira vez ou depois de uma reposição de fábrica, se não existir qualquer configuração de opções DHCP, o telefone contacta um servidor de ativação de dispositivos para aprovisionamento de toque zero. Os novos telefones utilizam "activate.cisco.com" em vez de "webapps.cisco.com" para aprovisionamento. Os telefones com versão de firmware anterior a 11.2(1) continuam a utilizar "webapps.cisco.com". Recomendamos que autorize ambos os nomes de domínio na sua firewall.

Passo 2 Selecione **Gestão de Certificados**.

No separador **Assinar CSR** o CSR do passo anterior está carregado para assinatura.

Passo 3 Na caixa de lista pendente **Selecionar Produto**, selecione **firmware SPA1xx 1.3.3 e mais recente/firmware SPA232D 1.3.3 e mais recente/firmware SPA5xx 7.5.6 e mais recente/CP-78xx-3PCC/CP-88xx-3PCC**.

Nota Este produto inclui os telefones multiplataforma Cisco IP Phone série 6800

Passo 4 No campo **Ficheiro CSR**, clique em **Procurar** e selecione o CSR para assinar.

Passo 5 Selecione o método de encriptação:

- MD5
- SHA1
- SHA256

A Cisco recomenda que selecione encriptação SHA256.

Passo 6 Na caixa de lista pendente **Duração da sessão**, selecione a duração aplicável (por exemplo, 1 ano).

Passo 7 Clique em **Assinar pedido de certificado**.

Passo 8 Selecione uma das seguintes opções para receber o certificado assinado:

- **Introduzir o endereço de e-mail do destinatário** — se pretender receber o certificado via e-mail, introduza o seu endereço de e-mail neste campo.
- **Transferir** — se pretender transferir o certificado assinado, selecione esta opção.

Passo 9 Clique em **Submit** (Submeter).

O certificado de servidor assinado é transferido ou enviado por e-mail para o endereço de e-mail anteriormente fornecido.

Certificado de raiz de cliente de autoridade de certificação de telefone multiplataforma

A Cisco também oferece um Certificado de raiz de cliente de autoridade de certificação de telefone multiplataforma ao provedor de serviços. Este certificado de raiz certifica a autenticidade do certificado de cliente de cada telefone. Os telefones multiplataforma também suportam certificados assinados por terceiros, como os fornecidos pela Verisign, Cybertrust e outras.

O certificado de cliente exclusivo que cada dispositivo oferece durante uma sessão HTTPS tem informações de identificação incorporadas no campo de assunto. Estas informações podem ser disponibilizadas pelo servidor HTTPS a um script CGI chamado para tratar de pedidos seguros. Especificamente, o assunto do certificado indica o nome de produto (elemento OU), o endereço MAC (elemento S) e o número de série (elemento L) da unidade.

O exemplo que se segue do campo de assunto do certificado de cliente dos telefones multiplataforma Cisco IP Phone 6841 mostra estes elementos:

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

Para determinar se um telefone tem um certificado individualizado, utilize a variável macro de aprovisionamento $CCERT. O valor da variável expande para Instalado ou Não instalado, segundo a presença ou ausência de um certificado de cliente exclusivo. No caso de um certificado genérico, é possível obter o número de série da unidade a partir do cabeçalho de pedido HTTP no campo Utilizador-Agente.

É possível configurar os servidores HTTPS para pedir certificados SSL a clientes com ligação. Se esta configuração estiver ativada, o servidor pode utilizar Certificado de raiz de cliente de autoridade de certificação de telefone multiplataforma fornecido pela Cisco para verificar o certificado do cliente. O servidor pode então fornecer as informações de certificado a uma CGI para processamento adicional.

A localização do armazenamento do certificado pode variar. Por exemplo, numa instalação Apache, os caminhos de ficheiro para armazenamento do certificado assinado pelo servidor de aprovisionamento, a respetiva chave privada associada e o Certificado de raiz de cliente de autoridade de certificação de telefone multiplataforma são os seguintes:

```
# 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
```

Para obter informações específicas, consulte a documentação de um servidor HTTPS.

A Autoridade de raiz de certificado de cliente Cisco assina cada certificado exclusivo. O certificado raiz correspondente é disponibilizado aos provedores de serviços para fins de autenticação de clientes.

Servidores redundantes de aprovisionamento

O servidor de aprovisionamento pode ser especificado como endereço IP ou como um nome de domínio completamente qualificado (FQDN). A utilização de um FQDN facilita a implementação de servidores de aprovisionamento redundantes. Quando o servidor de aprovisionamento é identificado através de um FQDN, o telefone tenta resolver o FQDN para um endereço IP através de DNS. Só são suportados registos A de DNS para aprovisionamento; a resolução de endereço DNS SRV não está disponível para aprovisionamento. O telefone continua a processar registos A até um servidor responder. Se nenhum servidor associado com os registos A responder, o telefone regista um erro ao servidor syslog.

Servidor syslog

Se um servidor syslog estiver configurado no telefone através da utilização dos parâmetros <Servidor Syslog>, as operações de ressincronização e atualização enviam mensagens para o servidor syslog. Uma mensagem pode ser gerada no início de um pedido de ficheiro remoto (perfil de configuração ou carga de carregamento firmware) e no final da operação (indicando sucesso ou falha).

As mensagens registadas são configuradas nos seguintes parâmetros e expandidas via macro para as mensagens efetivas do syslog:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

CAPÍTULO 4

Exemplos de aprovisionamento

Descrição geral de exemplos de aprovisionamento

Este capítulo oferece exemplos de procedimentos para a transferência de perfis de configuração entre o telefone e o servidor de aprovisionamento.

Para obter informações sobre a criação de perfis de configuração, consulte Aprovisionamento de scripts, na página 13.

Ressincronização básica

Esta secção demonstra a funcionalidade básica de ressincronização dos telefones.

Ressincronização TFTP

O telefone suporta vários protocolos de rede para recuperar perfis de configuração. O protocolo de transferência de perfil mais básico é TFTP (RFC1350). TFTP é amplamente utilizado para o aprovisionamento de dispositivos de rede em redes LAN privadas. Embora não recomendado para a implementação de terminais remotos através da Internet, TFTP pode ser conveniente para implementação em pequenas empresas, para pré-aprovisionamento interno e para desenvolvimento e testes. Consulte Pré-aprovisionamento interno do dispositivo, na página 41 para obter mais informações sobre pré-aprovisionamento interno. No procedimento que se segue, um perfil é modificado após transferir um arquivo de um servidor TFTP.

Procedure

Passo 1 Dentro de um ambiente LAN, ligue um PC e um telefone a um hub, comutador ou router pequeno.

Passo 2 No PC, instale e ative um servidor TFTP.

Passo 3 Utilize um editor de texto para criar um perfil de configuração que define o valor de GPP_A para 12345678, conforme indicado no exemplo.

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

Passo 4 Guarde o perfil com o nome `basic.txt` no diretório raiz do servidor TFTP.

Pode verificar se o servidor TFTP está corretamente configurado: peça o ficheiro `basic.txt` utilizando um cliente TFTP que não seja o telefone. Preferencialmente, utilize um cliente TFTP que esteja em execução num anfitrião independente do servidor de aprovisionamento.

Passo 5 Abra o web browser do PC na página de configuração admin/avançado. Por exemplo, se o endereço IP do telefone for 192.168.1.100:

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

Passo 6 Selecione o separador **Voz** > **Aprovisionamento** e inspecione os valores dos parâmetros genéricos GPP_A a GPP_P. Estes devem estar vazios.

Passo 7 Ressincronize o telefone de teste para o perfil de configuração `basic.txt` abrindo a URL de ressincronização numa janela do web browser.

Se o endereço IP do servidor TFTP for 192.168.1.200, o comando deve ser semelhante ao seguinte exemplo:

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

Quando o telefone recebe este comando, o dispositivo no endereço 192.168.1.100 pede o ficheiro `basic.txt` ao servidor TFTP no endereço IP 192.168.1.200. O telefone, em seguida, analisa o ficheiro transferido e atualiza o parâmetro GPP_A com o valor 12345678.

Passo 8 Verifique se o parâmetro foi corretamente atualizado: atualize a página de configuração no web browser do PC e selecione o separador **Voz** > **Aprovisionamento**.

O parâmetro GPP_A deve agora conter o valor 12345678.

Utilizar syslog para registar mensagens

O telefone envia uma mensagem de syslog para o servidor syslog designado quando o dispositivo está prestes a ressincronizar com um servidor de aprovisionamento e depois de a ressincronização estar concluída ou falhar. Para identificar este servidor é possível aceder à página da Web da administração do telefone (consulte Aceder à página da Web do telefone, na página 7), selecionar **Voz** > **Sistema** e identificar o servidor no parâmetro **Servidor Syslog** da secção **Configuração da rede opcional**. Configure o endereço IP do servidor syslog no dispositivo e observe as mensagens geradas durante os procedimentos restantes.

Procedure

Passo 1 Instalar e ativar um servidor syslog no PC local.

Passo 2 Programar o endereço IP do PC no parâmetro Syslog_Server do perfil e enviar a alteração:

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

Passo 3 Clique no separador **Sistema** e introduza o valor do seu servidor syslog local no parâmetro Syslog_Server.

Passo 4 Repita a operação de ressincronização conforme descrito em Ressincronização TFTP, na página 49.

O dispositivo gera duas mensagens do syslog durante a ressincronização. A primeira mensagem indica que está em curso um pedido. A segunda mensagem marca o sucesso ou falha da ressincronização.

Passo 5 Verifique se o servidor syslog recebeu mensagens semelhantes à seguinte:

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

Estão disponíveis mensagens detalhadas ao programar um parâmetro de Debug_Server (em vez do parâmetro Syslog_Server) com o endereço IP do servidor syslog, e ao definir o Debug_Level para um valor entre 0 e 3 (sendo 3 o mais detalhado):

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

O conteúdo destas mensagens pode ser configurado utilizando os seguintes parâmetros:

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Se qualquer um destes parâmetros for limpo, a mensagem de syslog correspondente não é gerada.

Ressincronizar um dispositivo automaticamente

Um dispositivo pode ressincronizar periodicamente com o servidor de aprovisionamento para garantir que todas as alterações de perfil feitas no servidor são propagadas para o dispositivo ponto final (em vez de enviar um pedido explícito de ressincronização para o ponto final).

Para fazer com que o telefone ressincronize periodicamente com um servidor, é definido um URL de perfil de configuração utilizando o parâmetro Profile_Rule e um período de ressincronização utilizando o parâmetro Resync_Periodic.

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Selecione **Voz** > **Aprovisionamento**.

Passo 2 Defina o parâmetro Profile_Rule. Este exemplo supões que o endereço IP do servidor TFTP é 192.168.1.200.

Passo 3 No campo **Ressincronização periódica**, insira um valor pequeno para teste, como **30** segundos.

Passo 4 Clique em **Submeter todas as alterações**.

Com as novas configurações de parâmetros, o telefone ressincroniza com o ficheiro de configuração especificado pelo URL duas vezes por minuto.

Passo 5 Observe as mensagens resultantes no rastreamento syslog (conforme descrito na secção Utilizar syslog para registar mensagens, na página 50).

Passo 6 Certifique-se de que o campo **Ressincronizar ao repor** está definido para **Sim**.

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

Passo 7 Desligue e volte a ligar o telefone para o forçar a ressincronizar com o servidor de aprovisionamento.

Se a operação de ressincronização falhar por qualquer motivo, como por exemplo se o servidor não responder, a unidade aguarda (durante o número de segundos configurado em **Atraso de repetição após erro na ressincronização**) antes de tentar ressincronizar novamente. Se o **Atraso de repetição após erro na ressincronização** for zero, o telefone não tenta ressincronizar após uma tentativa falhada de ressincronização.

Passo 8 (Opcional) Defina o valor do campo **Atraso de repetição após erro na ressincronização** para um número pequeno, como **30**.

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

Passo 9 Desative o servidor TFTP e observe os resultados na saída do syslog.

Perfis exclusivos, expansão via macro e HTTP

Numa implementação em que cada telefone deve ser configurado com valores distintos para alguns parâmetros, como User_ID ou Display_Name, o provedor de serviços pode criar um perfil exclusivo para cada dispositivo implementado e servir de anfitrião a esses perfis num servidor de aprovisionamento. Cada telefone, por sua vez, deve ser configurado para ressincronizar com o seu próprio perfil de acordo com uma convenção de nomenclatura de perfil predeterminada.

A sintaxe do URL do perfil pode incluir informações de identificação específicas para cada telefone, como o endereço MAC ou o número de série, utilizando a expansão macro de variáveis incorporadas. A expansão via macro elimina a necessidade de especificar estes valores em vários locais dentro de cada perfil.

Uma regra de perfil passa por expansão via macro antes de ser aplicada ao telefone. A expansão via macro controla diversos valores, por exemplo:

- $MA expande para o endereço MAC de 12 dígitos da unidade (com dígitos hexadecimais minúsculos). Por exemplo, 000e08abcdef.
- $SN expande para o número de série da unidade. Por exemplo, 88012BA01234.

É possível expandir outros valores via macro desta forma, incluindo todos os parâmetros genéricos, de GPP_A a GPP_P. Um exemplo deste processo pode ser visto em Ressincronização TFTP, na página 49. A expansão via macro não se limitada ao nome do ficheiro URL, podendo também ser aplicada a qualquer porção do

parâmetro de regra de perfil. Estes parâmetros são referidos como $A a $P. Para obter uma lista completa de variáveis disponíveis para expansão via macro, consulte Variáveis de expansão via macro, na página 74.

Neste exercício, um perfil específico de um telefone é aprovisionado num servidor TFTP.

Exercício: aprovisionar um perfil do telefone IP específico num servidor TFTP

Procedure

Passo 1 Obtenha o endereço MAC do telefone a partir da respetiva etiqueta de produto. (O endereço MAC é o número, com números e dígitos hexadecimais minúsculos, como 000e08aabbcc.

Passo 2 Copie o ficheiro de configuração `basic.txt` (descrito em Ressincronização TFTP, na página 49) para um novo ficheiro chamado `CP-xxxx-3PCC macaddress.cfg` (substituindo `xxxx` pelo número de modelo e `macaddress` pelo endereço MAC do telefone).

Passo 3 Mova o novo ficheiro no diretório raiz virtual do servidor TFTP.

Passo 4 Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Passo 5 Selecione **Voz** > **Aprovisionamento**.

Passo 6 Introduza `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` no campo **Regra de perfil**.

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

Passo 7 Clique em **Submeter todas as alterações**. Isto irá provocar uma reinicialização e ressincronização imediatas.

Quando ocorrer a próxima ressincronização, o telefone recupera o novo ficheiro expandindo a expressão macro $MA no respetivo endereço MAC.

Ressincronização HTTP GET

HTTP fornece um mecanismo de ressincronização mais fiável que TFTP, porque HTTP estabelece uma ligação TCP e TFTP utiliza o UDP menos fiável. Além disso, os servidores HTTP oferecem funcionalidades de registo e filtragem aperfeiçoados, em comparação com os servidores TFTP.

No lado do cliente, o telefone não exige qualquer configuração especial no servidor para poder ressincronizar utilizando HTTP. A sintaxe de parâmetro Profile_Rule para utilizar HTTP com o método GET é semelhante à sintaxe utilizada para TFTP. Se um web browser padrão puder recuperar um perfil do seu servidor HTTP, o telefone também deverá poder fazê-lo.

Exercício: ressincronização HTTP GET

Procedure

Passo 1 Instale um servidor HTTP no PC local ou noutro anfitrião acessível.

Pode transferir o servidor Apache open source da Internet.

Passo 2 Copie o perfil de configuração `basic.txt` (descrito em Ressincronização TFTP, na página 49) para o diretório raiz virtual do servidor instalado.

Passo 3 Para verificar a correta instalação do servidor e acesso do ficheiro a `basic.txt`, aceda ao perfil com um web browser.

Passo 4 Modifique o Profile_Rule do telefone de teste para apontar para o servidor HTTP em vez de servidor TFTP, para transferir o respetivo perfil periodicamente.

Por exemplo, partindo do princípio de que o servidor HTTP está em 192.168.1.300, introduza o seguinte valor:

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

Passo 5 Clique em **Submeter todas as alterações**. Isto irá provocar uma reinicialização e ressincronização imediatas.

Passo 6 Observe as mensagens syslog enviadas pelo telefone. As ressincronizações periódicas devem agora obter o perfil do servidor HTTP.

Passo 7 Nos registos do servidor HTTP, observe como as informações que identificam o telefone de teste aparecem no registo dos agentes de utilizador.

Estas informações devem incluir o fabricante, o nome do produto, a versão de firmware atual e o número de série.

Aprovisionamento através de Cisco XML

É possível aprovisionar através de funções Cisco XML para cada um dos telefones, designados aqui como xxxx.

É possível enviar um objeto XML para o telefone através de um pacote de notificação SIP ou um HTTP Post para a interface CGI do telefone: `http://IPAddressPhone/CGI/Execute`.

O CP-xxxx-3PCC estende a funcionalidade Cisco XML para suportar o aprovisionamento através de um objeto XML:

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

Depois de o telefone receber o objeto XML, ele transfere o ficheiro de aprovisionamento de [profile-rule]. Esta regra utiliza macros para simplificar o desenvolvimento da aplicação de serviços XML.

Resolução de URL com expansão via macro

O servidor tem subdiretórios com vários perfis que constituem um método conveniente para gerir um grande número de dispositivos implementados. O perfil de URL pode conter:

- Um nome de servidor de aprovisionamento ou um endereço IP explícito. Se o perfil identificar o servidor de aprovisionamento por nome, o telefone executa uma pesquisa DNS para resolver o nome.
- Uma porta do servidor não padrão especificada no URL utilizando a sintaxe padrão `:port` após o nome do servidor.

- O subdiretório do diretório raiz virtual do servidor onde o perfil está armazenado, especificado utilizando anotação de URL padrão e gerida pela expansão via macro.

Por exemplo, a Profile_Rule que se segue pede o ficheiro de perfil ($PN.cfg), no subdiretório do servidor `/cisco/config`, a partir do servidor TFTP executado no anfitrião prov.telco.com a aguardar uma ligação na porta 6900:

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

Pode ser identificado um perfil para cada telefone num parâmetro genérico, com o valor referido dentro de uma regra de perfil comum utilizando expansão via macro.

Por exemplo, supondo que GPP_B é definido como `Dj6Lmp23Q`.

O Profile_Rule tem o valor:

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

Quando o dispositivo ressincroniza e as macros são expandidas, o telefone com um endereço MAC de 000e08012345 pede o perfil com o nome que contém o endereço MAC do dispositivo no seguinte URL:

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

Ressincronização HTTPS segura

Estes mecanismos estão disponíveis no telefone para ressincronização com um processo de comunicação seguro:

- Ressincronização HTTPS básica
- HTTPS com autenticação de certificado de cliente
- Conteúdo dinâmico e filtragem de cliente HTTPS

Ressincronização HTTPS básica

HTTPS adiciona SSL a HTTP para aprovisionamento remoto para que:

- O telefone possa autenticar o servidor de aprovisionamento.
- O servidor de aprovisionamento possa autenticar o telefone.
- A confidencialidade das informações trocadas entre o telefone e o servidor de aprovisionamento seja assegurada.

SSL gera e troca chaves secretas (simétricas) para cada ligação entre o telefone e o servidor, utilizando os pares de chave pública/privada pré-instalados no telefone e no servidor de aprovisionamento.

No lado do cliente, o telefone não exige qualquer configuração especial do servidor para poder ressincronizar com HTTP. A sintaxe de parâmetro Profile_Rule para utilizar HTTPS com o método GET é semelhante à

sintaxe utilizada para HTTP ou TFTP. Se um web browser padrão puder recuperar um perfil do seu servidor HTTPS, o telefone também deverá poder fazê-lo.

Além de instalar um servidor HTTPS, deve ser instalado no servidor de aprovisionamento um certificado de servidor SSL assinado pela Cisco. Os dispositivos não podem ressincronizar com um servidor que utilize HTTPS, a menos que o servidor forneça um certificado de servidor assinado pela Cisco. As instruções para criar certificados SSL assinados para produtos de voz podem encontrar-se em https://supportforums.cisco.com/docs/DOC-9852.

Exercício: ressincronização HTTPS básica

Procedure

Passo 1 Instale um servidor HTTPS num anfitrião cujo endereço IP seja conhecido no servidor de DNS da rede através da tradução normal do nome de anfitrião.

O servidor Apache open source pode ser configurado para funcionar como servidor HTTPS quando instalado com o pacote open source mod_ssl.

Passo 2 Gere um pedido de assinatura do certificado do servidor ao servidor. Para este passo pode ser necessário instalar o pacote OpenSSL open source ou software equivalente. Se utilizar OpenSSL, o comando para gerar o ficheiro CSR básico é o seguinte:

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

Este comando gera um par de chaves pública/privada, que é guardado no ficheiro `privkey.pem`.

Passo 3 Envie o ficheiro CSR (provserver.csr) para a Cisco para assinatura.

É devolvido um certificado de servidor assinado (provserver.cert) juntamente com um Certificado de raiz de cliente de autoridade de certificação Sipura, spacroot.cert.

Consulte https://supportforums.cisco.com/docs/DOC-9852 para mais informações

Passo 4 Armazene o certificado de servidor assinado, o ficheiro do par de chaves privadas e o certificado raiz de cliente nas localizações adequadas no servidor.

No caso de uma instalação Apache em Linux, estas localizações são normalmente as seguintes:

```
# 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
```

Passo 5 Reinicie o servidor.

Passo 6 Copie o ficheiro de configuração `basic.txt` (descrito em Ressincronização TFTP, na página 49) para o diretório raiz virtual do servidor HTTPS.

Passo 7 Verifique o funcionamento devido do servidor transferindo `basic.txt` do servidor HTTPS com um browser padrão a partir do PC local.

Passo 8 Inspecione o certificado de servidor fornecido pelo servidor.

O browser provavelmente não reconhece o certificado como válido, a menos que o navegador tenha sido pré-configurado para aceitar a Cisco como uma Autoridade de Certificação raiz. No entanto, os telefones esperam que o certificado seja assinado desta forma.

Modifique a Profile_Rule do dispositivo de teste para conter uma referência ao servidor HTTPS, por exemplo:

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

Este exemplo parte do princípio de que o nome do servidor HTTPS é **`my.server.com`**.

Passo 9 Clique em **Submeter todas as alterações**.

Passo 10 Observe o rastreamento de syslog enviado pelo telefone.

A mensagem de syslog deve indicar que a ressincronização obteve o perfil do servidor HTTPS.

Passo 11 (Opcional) Utilize um analisador de protocolo de Ethernet na sub-rede do telefone para verificar que os pacotes estão encriptados.

Neste exercício não foi ativada a verificação do certificado de cliente. A ligação entre o telefone e servidor está encriptada. No entanto, a transferência não é segura porque qualquer cliente pode ligar-se ao servidor e pedir o ficheiro, desde que saiba o nome do ficheiro e a localização do diretório. Para uma ressincronização segura, o servidor também deve autenticar o cliente, conforme demonstrado no exercício descrito em HTTPS com autenticação de certificado de cliente, na página 57.

HTTPS com autenticação de certificado de cliente

Na configuração predefinida de fábrica, o servidor não pede um certificado de cliente SSL a um cliente. A transferência do perfil não é segura porque qualquer cliente pode ligar-se ao servidor e pedir o perfil. Pode editar a configuração para ativar a autenticação de cliente; o servidor exige um certificado de cliente para autenticar o telefone antes de aceitar um pedido de ligação.

Devido a esta exigência, a operação de ressincronização não pode ser testada independentemente usando um browser que não tenha as credenciais adequadas. É possível observar a troca de chaves de SSL dentro da ligação HTTPS entre o telefone de teste e o servidor com o utilitário ssldump. O rastreamento do utilitário mostra a interação entre cliente e servidor.

Exercício: HTTPS com autenticação de certificado de cliente

Procedure

Passo 1 Ative a autenticação de certificado de cliente no servidor HTTPS.

Passo 2 No Apache (v.2), defina o seguinte no servidor do ficheiro de configuração:

```
SSLVerifyClient  require
```

Além disso, certifique-se de que spacroot.cert foi armazenado conforme indicado no exercício Ressincronização HTTPS básica, na página 55.

Passo 3 Reinicie o servidor HTTPS e observe o rastreamento de syslog do telefone.

Cada ressincronização com o servidor executa agora autenticação simétrica, e o certificado do servidor e o certificado de cliente são verificados antes do perfil ser transferido.

Passo 4 Utilize ssldump para capturar uma ligação de ressincronização entre o telefone e o servidor HTTPS.

Se a verificação de certificado de cliente estiver devidamente ativada no servidor, o rastreamento de ssldump mostra a troca simétrica de certificados (primeiro do servidor para o cliente, depois do cliente para o servidor) antes dos pacotes encriptados que contêm o perfil.

Com a autenticação de cliente ativada, só um telefone com um endereço MAC correspondente a um certificado de cliente válido pode solicitar o perfil do servidor de aprovisionamento. O servidor rejeita um pedido de um browser comum ou de outro dispositivo não autorizado.

Conteúdo dinâmico e filtragem de cliente HTTPS

Se o servidor HTTPS estiver configurado para exigir um certificado de cliente, as informações no certificado identificam o telefone a ressincronizar e fornecem-lhe as informações de configuração corretas.

O servidor HTTPS disponibiliza as informações de certificado para scripts CGI (ou programas CGI compilados) que são chamados como parte do pedido de ressincronização. Para efeitos de ilustração, este exercício utiliza a linguagem de script open source Perl, e parte do princípio de que Apache (v.2) é utilizado como servidor HTTPS.

Procedure

Passo 1 Instale Perl no anfitrião que executa o servidor HTTPS.

Passo 2 Gere o seguinte script refletor 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>";
```

Passo 3 Guarde este ficheiro com o nome de ficheiro `reflect.pl`, com permissão executável (chmod 755 em Linux), no diretório de scripts CGI do servidor HTTPS.

Passo 4 Verifique a acessibilidade dos scripts CGI no servidor (ou seja, `/cgi-bin /...`).

Passo 5 Modifique Profile_Rule no dispositivo de teste para ressincronizar com o script refletor, como no seguinte exemplo:

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

Passo 6 Clique em **Submeter todas as alterações**.

Passo 7 Observe o rastreamento de syslog para garantir uma ressincronização bem-sucedida.

Passo 8 Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Passo 9 Selecione **Voz** > **Aprovisionamento**.

Passo 10 Verifique se o parâmetro GPP_D contém as informações capturadas pelo script.

Estas informações contêm o nome do produto, o endereço MAC e o número de série se o dispositivo de teste tiver um certificado exclusivo do fabricante. As informações contêm cadeias de caracteres genéricas se a unidade tiver sido fabricada antes da versão 2.0 do firmware.

Um script semelhante pode determinar informações sobre o dispositivo em a ressincronizar e, em seguida, fornecer ao dispositivo os valores de parâmetro de configuração adequados.

Certificados HTTPS

O telefone fornece uma estratégia de aprovisionamento segura e fiável com base nos pedidos HTTPS do dispositivo ao servidor de aprovisionamento. São utilizados um certificado de servidor e um certificado de cliente para autenticar o telefone no servidor e o servidor no telefone.

Para usar HTTPS com o telefone, deve gerar um pedido de assinatura de certificado (CSR) e enviá-lo à Cisco. O telefone gera um certificado para instalação no servidor de aprovisionamento. O telefone aceita o certificado quando procura estabelecer uma ligação HTTPS ao servidor de aprovisionamento.

Metodologia HTTPS

HTTPS encripta a comunicação entre um cliente e um servidor, protegendo assim o conteúdo da mensagem de outros dispositivos de rede. O método de encriptação para o corpo da comunicação entre um cliente e um servidor baseia-se em encriptação de chave simétrica. Com encriptação de chave simétrica, um cliente e um servidor partilham uma única chave secreta através de um canal seguro protegido por encriptação de chave pública/privada.

As mensagens encriptadas pela chave secreta só podem ser desencriptadas utilizando a mesma chave. HTTPS suporta uma ampla gama de algoritmos de encriptação simétricos. O telefone implementa até 256 bits de encriptação simétrica, utilizando a norma de encriptação americana (AES), além de RC4 de 128 bits.

HTTPS também contribui para a autenticação de um servidor e cliente envolvidos numa transação segura. Esta funcionalidade garante que um servidor de aprovisionamento e um cliente individual não podem ser simulados por outros dispositivos na rede. Esta funcionalidade é essencial no contexto de aprovisionamento do ponto final remoto.

A autenticação de servidor e cliente é efetuada através de encriptação de chave pública/privada com um certificado que contém a chave pública. O texto encriptado com uma chave pública só pode ser desencriptado pela chave privada correspondente (e vice-versa). O telefone suportar o algoritmo Rivest-Shamir-Adleman (RSA) para encriptação de chave pública/privada.

Certificado de servidor SSL

Cada servidor de aprovisionamento seguro recebe um certificado de servidor secure sockets layer (SSL) diretamente assinado pela Cisco. O firmware executado no telefone só reconhece como válidos os certificados da Cisco. Quando um cliente se liga a um servidor através de HTTPS, ele rejeita qualquer certificado de servidor não assinado pela Cisco.

Este mecanismo protege o provedor de serviços de acessos não autorizados ao telefone, ou de qualquer tentativa de simulação do servidor de aprovisionamento. Sem essa proteção, um atacante pode conseguir re-aprovisionar o telefone para obter informações de configuração, ou utilizar um serviço de VoIP diferente. Sem a chave privada que corresponde a um certificado de servidor válido, o atacante não consegue estabelecer comunicação com um telefone.

Obter um certificado de servidor

Procedure

Passo 1 Entre em contacto com uma pessoa de suporte da Cisco que irá colaborar consigo no processo de certificado. Se não estiver em colaboração com uma pessoa de suporte específica, envie o seu pedido por e-mail para ciscosb-certadmin@cisco.com.

Passo 2 Gere uma chave privada que irá ser utilizada num CSR (pedido de assinatura de certificado). Esta chave é privada e não é necessário fornecê-la ao suporte da Cisco. Use o "openssl" open source para gerar a chave. Por exemplo:

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

Passo 3 Gere um CSR que contém os campos que identificam a sua empresa e localização. Por exemplo:

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

É necessário ter as seguintes informações:

- Campo assunto - Introduza o nome comum (CN) que deve ter uma sintaxe FQDN (nome de domínio totalmente qualificado). Durante o handshake de autenticação do SSL, o telefone verifica se o certificado recebido vem da máquina que o apresentou.
- Nome de anfitrião do servidor - Por exemplo, provserv.domain.com.
- Endereço de email - Introduza um endereço de e-mail para que o suporte ao cliente possa entrar em contacto consigo, se necessário. Este endereço de e-mail é visível no CSR.

Passo 4 Envie o CSR (em formato de ficheiro zip) para a pessoa do suporte Cisco ou para ciscosb-certadmin@cisco.com. O certificado é assinado pela Cisco. A Cisco envia o certificado para instalar no seu sistema.

Certificado de cliente

Além de um ataque direto a um telefone, um atacante pode tentar contactar um servidor de aprovisionamento através de um web browser padrão ou outro cliente HTTPS para obter o perfil de configuração do servidor de aprovisionamento. Para evitar este tipo de ataques, cada telefone também tem um certificado de cliente exclusivo, assinado pela Cisco, que inclui informações de identificação sobre cada ponto final individual. É atribuído a cada provedor de serviços um certificado de raiz de autoridade de certificação com capacidade para autenticar o certificado de cliente do dispositivo. Este caminho de autenticação permite ao servidor de aprovisionamento rejeitar pedidos não autorizados de perfis de configuração.

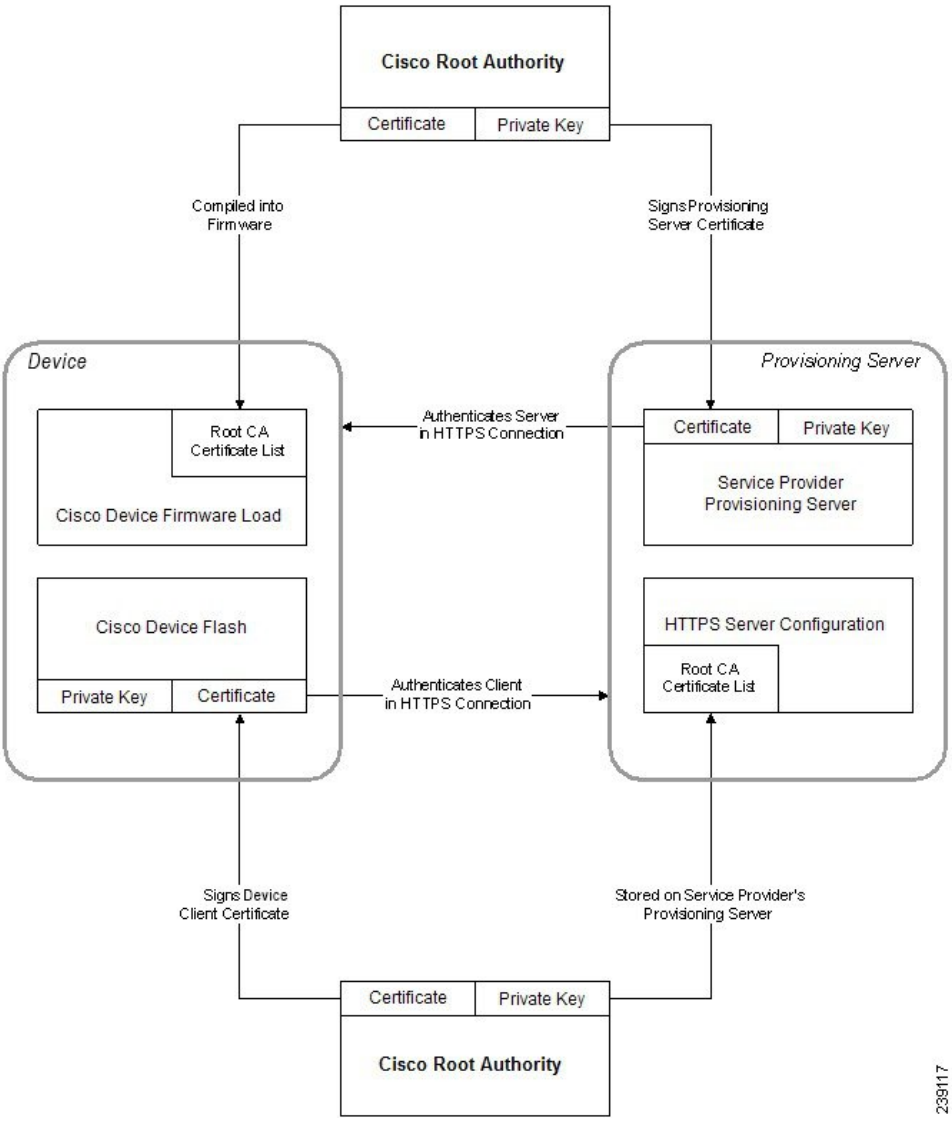
Estrutura de certificado

A combinação de um certificado de servidor e um certificado de cliente garante a comunicação segura entre um telefone remoto e o respetivo servidor de aprovisionamento. A figura abaixo ilustra a relação e colocação

de certificados, pares de chave pública/privada e autoridades de raiz de assinatura, entre o cliente Cisco, o servidor de aprovisionamento e a autoridade de certificação.

A metade superior do diagrama indica a Autoridade de raiz do servidor de aprovisionamento utilizada para assinar o certificado do servidor de aprovisionamento individual. O certificado de raiz correspondente é compilado para o firmware, o que permite ao telefone autenticar servidores de aprovisionamento autorizados.

Figura 2: Fluxo de Autoridade de Certificação



Configurar uma autoridade de certificação personalizada

É possível utilizar certificados digitais para autenticar dispositivos de rede e utilizadores na rede. Podem ser utilizados para negociar sessões de IPSec entre os nós de rede.

Um terceiro utiliza um certificado de Autoridade de Certificação para validar e autenticar dois ou mais nós que estão a tentar comunicar. Cada nó tem uma chave pública e privada. A chave pública encripta os dados.

A chave privada desencripta os dados. Uma vez que os nós obtiveram os respetivos certificados da mesma fonte, as respetivas identidades são garantidas.

O dispositivo pode utilizar certificados digitais fornecidos por uma Autoridade de Certificação (CA) de terceiros para autenticar ligações IPSec.

Os telefones suportam um conjunto de Autoridade de Certificação Raiz pré-carregado incorporado no firmware:

- Certificado de Autoridade de Certificação para pequenas empresas Cisco
- Certificado de Autoridade de Certificação CyberTrust
- Certificado de Autoridade de Certificação VeriSign
- Certificado de Autoridade de Certificação raiz Sipura
- Certificado de Autoridade de Certificação raiz Linksys

Before you begin

Aceda à página da Web da administração do telefone. Consulte Aceder à página da Web do telefone, na página 7.

Procedure

Passo 1 Selecione **Informações** > **Estado**.

Passo 2 Desloque-se até **Estado de Autoridade de Certificação personalizada** e veja os seguintes campos:

- Estado de aprovisionamento de Autoridade de Certificação personalizada — indica o estado do aprovisionamento.
  - Último aprovisionamento com êxito em mm/dd/aaaa HH:MM:SS; ou
  - Último aprovisionamento falhou em mm/dd/aaaa HH:MM:SS
- Informações de Autoridade de Certificação personalizada — Apresenta informações sobre a Autoridade de Certificação personalizada.
  - Instalado — Apresenta o "Valor de CN", em que "Valor de CN" é o valor do parâmetro CN do campo Assunto no primeiro certificado.
  - Não instalado — Apresentado se não estiver instalado qualquer certificado de Autoridade de Certificação personalizada.

Gestão de perfil

Esta secção demonstra a formação de perfis de configuração na preparação para transferência. Para explicar a funcionalidade, utiliza-se TFTP de um computador local como método de ressincronização, embora também se possa utilizar HTTP ou HTTPS.

Comprimir um perfil aberto com Gzip

Um perfil de configuração em formato XML pode ficar muito grande, se o perfil especificar todos os parâmetros individualmente. Para reduzir a carga sobre o servidor de aprovisionamento, o telefone suporta a compressão do ficheiro XML, utilizando o formato de compressão deflate suportado pelo utilitário gzip (RFC 1951).

Nota A compressão deve preceder a encriptação para que o telefone reconheça um perfil XML comprimido e encriptado.

Para integração com soluções de servidor de aprovisionamento back-end personalizadas, pode utilizar-se a biblioteca de compressão open source zlib em vez do utilitário independente gzip para executar a compressão do perfil. No entanto, o telefone espera que o ficheiro contenha um cabeçalho gzip válido.

Procedure

Passo 1 Instale o gzip no PC local.

Passo 2 Comprima o perfil de configuração `basic.txt` (descrito em Ressincronização TFTP, na página 49) chamando o gzip a partir da linha de comando:

```
gzip basic.txt
```

Esta ação gera o ficheiro deflated `basic.txt.gz`.

Passo 3 Guarde o ficheiro `basic.txt.gz` no diretório raiz virtual do servidor TFTP.

Passo 4 Modifique o Profile_Rule no dispositivo de teste para ressincronizar com o ficheiro deflated em vez do ficheiro XML original, conforme indicado no exemplo a seguir:

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

Passo 5 Clique em **Submeter todas as alterações.**

Passo 6 Observe o rastreamento de syslog do telefone.

Após a ressincronização, o telefone transfere o novo ficheiro e utiliza-o para atualizar os respetivos parâmetros.

Tópicos relacionados

Compressão de perfil aberto, na página 18

Encriptar um perfil com OpenSSL

É possível encriptar um perfil comprimido ou descomprimido (no entanto, é necessário comprimir um ficheiro antes de o encriptar). A encriptação é útil quando a confidencialidade das informações do perfil for particularmente importante, como quando se utiliza TFTP ou HTTP para a comunicação entre o telefone e o servidor de aprovisionamento.

O telefone suporta encriptação de chave simétrica com o algoritmo AES de 256 bits. Esta encriptação pode ser executada com o pacote de OpenSSL open source.

Procedure

Passo 1 Instale o OpenSSL num PC local. Esta ação pode exigir a recompilação da aplicação OpenSSL para ativar AES.

Passo 2 Com o ficheiro de configuração `basic.txt` (descrito em Ressincronização TFTP, na página 49), gere um ficheiro encriptado com o seguinte comando:

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

Também é possível utilizar o ficheiro `basic.txt.gz` comprimido criado em Comprimir um perfil aberto com Gzip, na página 63, porque o perfil XML pode ser comprimido e encriptado.

Passo 3 Guarde o ficheiro encriptado `basic.cfg` no diretório raiz virtual do servidor TFTP.

Passo 4 Modifique Profile_Rule no dispositivo de teste para ressincronizar com o ficheiro encriptado em vez do ficheiro XML original. A chave de encriptação é divulgada ao telefone com a seguinte opção de URL:

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

Passo 5 Clique em **Submeter todas as alterações**.

Passo 6 Observe o rastreamento de syslog do telefone.

Após a ressincronização, o telefone transfere o novo ficheiro e utiliza-o para atualizar os respetivos parâmetros.

Tópicos relacionados

Encriptação AES-256-CBC, na página 19

Criar perfis particionados

Um telefone transfere vários perfis separados durante cada ressincronização. Esta prática permite que a gestão de diferentes tipos de informações de perfil em servidores separados e a manutenção de valores de parâmetros de configuração do comuns separados de valores específicos de conta.

Procedure

Passo 1 Crie um novo perfil XML, `basic2.txt`, que especifica um valor de um parâmetro que o torna diferente dos exercícios anteriores. Por exemplo, para o perfil `basic.txt`, adicione o seguinte:

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

Passo 2 Armazene o perfil `basic2.txt` no diretório raiz virtual do servidor TFTP.

Passo 3 Deixe a primeira regra de perfil dos exercícios anteriores na pasta, mas configure a segunda regra de perfil (Profile_Rule_B) para apontar para o novo ficheiro:

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

```
</Profile_Rule_B>
```

Passo 4 Clique em **Submeter todas as alterações**.

O telefone ressincroniza agora para o primeiro e para o segundo perfil, por essa ordem, sempre que for altura de ressincronizar.

Passo 5 Observe o rastreamento de syslog para confirmar o comportamento esperado.

Definir o cabeçalho de privacidade do telefone

Um cabeçalho de privacidade do utilizador na mensagem SIP define as necessidades de privacidade do utilizador relativamente à rede fidedigna.

Pode definir o valor do cabeçalho de privacidade do utilizador para cada extensão da linha utilizando uma etiqueta XML no ficheiro `config.xml`.

As opções de cabeçalho de privacidade são:

- Desativado (predefinição)
- nenhum — o utilizador solicita que um serviço de privacidade não aplique funções de privacidade a esta mensagem SIP.
- cabeçalho — o utilizador necessita que um serviço de privacidade oculte cabeçalhos dos quais não é possível eliminar informações de identificação.
- sessão — o utilizador solicita que um serviço de privacidade forneça anonimato para as sessões.
- utilizador — o utilizador solicita um nível de privacidade apenas através de intermediários.
- id — o utilizador solicita que o sistema substitua um ID que não revela o endereço IP ou nome de anfitrião.

Procedure

Passo 1 Edite o ficheiro `config.xml` do telefone num editor de texto ou XML.

Passo 2 Insira a etiqueta **<Privacy_Header_N_ ua="na">*Valor*</Privacy_Header_N_>**, em que N é o número de extensão (1–10), e utilize um dos seguintes valores.

- Valor predefinido: **Desativado**
- **none**
- **informação prévia**
- **sessão**
- **user**
- **ID**

Passo 3 (Opcional) Aprovisione quaisquer extensões de linha de adição utilizando a mesma etiqueta com o número de extensão da linha necessária.

Passo 4 Guarde as alterações ao ficheiro `config`.

CAPÍTULO 5

Parâmetros de aprovisionamento

Descrição geral dos parâmetros de aprovisionamento

Este capítulo descreve os parâmetros de aprovisionamento que podem ser utilizados em scripts de perfil de configuração.

Parâmetros de configuração de perfil

A tabela que se segue define a função e utilização de cada parâmetro na secção **Parâmetros de configuração de perfil** do separador **Aprovisionamento**.

Nome do parâmetro	Descrição e o valor predefinido
Ativar provisão	Controla todas as ações de ressincronização independentemente das ações de atualização do firmware. Defina como **Sim** para ativar o aprovisionamento remoto. O valor predefinido é Sim.
Ressincronizar ao repor	Aciona uma ressincronização após cada reinicialização, exceto reinicializações causadas por atualizações de parâmetros atualizações e de firmware. O valor predefinido é Sim.

Nome do parâmetro	Descrição e o valor predefinido
Ressincronizar com atraso aleatório	Um atraso aleatório depois da a sequência de inicialização antes de executar a reposição, especificado em segundos. Num conjunto de dispositivos de telefonia IP agendados para ligar em simultâneo, este comando introduz uma dispersão nas horas a que cada unidade envia um pedido de ressincronização ao servidor de aprovisionamento. Esta funcionalidade pode ser útil numa implementação residencial grande, no caso de uma falha de energia regional. O valor para este campo tem de ser um número inteiro entre 0 e 65535. O valor predefinido é 2.
Ressincronizar às (HHmm)	O tempo (HHmm) a que o dispositivo ressincroniza com o servidor de aprovisionamento. O valor para este campo tem de ser um número de quatro dígitos desde 0000 até 2400 para indicar o tempo em formato HHmm. Por exemplo, 0959 indica 09:59. O valor predefinido é vazio. Se o valor for inválido, o parâmetro é ignorado. Se este parâmetro estiver configurado com um valor válido, o parâmetro Ressincronização periódica é ignorado.
Ressincronizar com atraso aleatório	Evita uma sobrecarga do servidor de aprovisionamento quando um grande número de dispositivos liga simultaneamente. Para evitar inundar o servidor com pedidos de ressincronização de vários telefones, o telefone ressincroniza no intervalo entre as horas e minutos e as horas e minutos mais o atraso aleatório (hhmm, hhmm + random_delay). Por exemplo, se o atraso aleatório = (Ressincronizar com atraso aleatório + 30)/60 minutos, o valor de introdução em segundos é convertido em minutos, arredondando para o minuto seguinte, para calcular o intervalo random_delay final. Os intervalos de valor válido entre 0 e 65535. Esta funcionalidade está desativada quando este parâmetro está definido como zero. O valor predefinido é de 600 segundos (10 minutos).

Nome do parâmetro	Descrição e o valor predefinido
Ressincronização periódica	O intervalo de tempo entre as ressincronizações periódicas com o servidor de aprovisionamento. O temporizador de ressincronização associado está ativo apenas depois da primeira sincronização bem-sucedida com o servidor. Os formatos válidos são os seguintes: • Um inteiro Exemplo: uma introdução de **`3000`** indica que a ressincronização seguinte ocorre em 3000 segundos. • Vários inteiros Exemplo: uma introdução de **`600,1200,300`** indica que a primeira ressincronização ocorre em 600 segundos, a segunda ressincronização ocorre 1200 segundos após a primeira e a terceira ressincronização ocorre 300 segundos após a segunda. • Um intervalo de tempo Exemplo: uma introdução de **`2400+30`** indica que a ressincronização seguinte ocorre entre 2400 e 2430 segundos após uma ressincronização bem sucedida. Defina este parâmetro como zero para desativar a ressincronização periódica. O valor predefinido é 3600 segundos.

Nome do parâmetro	Descrição e o valor predefinido
Atraso de repetição após erro na ressincronização	Se uma operação de ressincronização falhar porque o dispositivo de telefonia IP não conseguiu recuperar um perfil do servidor, ou porque o ficheiro transferido está corrompido, ou se ocorrer um erro interno, o dispositivo tenta ressincronizar novamente após um tempo especificado em segundos. Os formatos válidos são os seguintes: • Um inteiro Exemplo: uma introdução de **300** indica que a próxima tentativa de ressincronização ocorre em 300 segundos. • Vários inteiros Exemplo: uma introdução de **600,1200,300** indica que a primeira repetição ocorre 600 segundos após a falha, a segunda repetição ocorre 1200 segundos após a falha da primeira repetição e a terceira repetição ocorre 300 segundos após a falha da segunda repetição. • Um intervalo de tempo Exemplo: uma introdução de **2400+30** indica que a próxima repetição ocorre entre 2400 e 2430 segundos após uma falha de ressincronização. Se o atraso estiver definido para 0, o dispositivo não tenta ressincronizar novamente após uma tentativa falhada de ressincronização.
Atraso de ressincronização forçado	Atraso máximo (em segundos) do telefone antes de efetuar uma ressincronização. O dispositivo não ressincroniza enquanto uma das respetivas linhas de telefone estiver ativa. Uma vez que uma ressincronização pode demorar vários segundos, é aconselhável esperar até o dispositivo estar inativo durante um período alargado antes de ressincronizar. Isto permite ao utilizador efetuar chamadas consecutivas sem interrupções. O dispositivo tem um temporizador que começa a contagem decrescente quando todas as respetivas linhas estão inativas. Este parâmetro é o valor inicial do contador. Os eventos de ressincronização são atrasados até este contador ficar a zero. Os intervalos de valor válido entre 0 e 65535. O valor predefinido é de 14,400 segundos.

Nome do parâmetro	Descrição e o valor predefinido
Ressincronizar de SIP	Permite o acionamento de uma ressincronização através de uma mensagem SIP NOTIFY. O valor predefinido é Sim.
Ressincronizar após a tentativa de atualização	Ativa ou desativa a operação de ressincronização após ter ocorrido qualquer atualização. Se for selecionado Sim, é acionada a sincronização. O valor predefinido é Sim.
Acionador 1 de ressincronização, Acionador 2 de ressincronização	Condições configuráveis de acionador de ressincronização. Uma ressincronização é acionada quando a equação lógica nestes parâmetros é avaliada como TRUE. O valor predefinido é (vazio).
Ressincronizar quando FNF	Uma ressincronização é considerada sem êxito se um perfil pedido não for recebido do servidor. Este parâmetro pode substituir essa situação. Quando está definido como **não**, o dispositivo aceita uma resposta de `ficheiro não encontrado` do servidor como uma ressincronização bem sucedida. O valor predefinido é Sim.
Regra do perfil Regra B do perfil Regra C do perfil Regra D do perfil	Cada regra de perfil informa o telefone de uma fonte a partir da qual obter um perfil (ficheiro de configuração). Durante cada operação de ressincronização, o telefone aplica todos os perfis em sequência. Predefinição: **`/$PSN.xml`** Se estiver a aplicar encriptação AES-256-CBC aos ficheiros de configuração, especifique a chave de encriptação com a palavra-chave **`--key`** da seguinte forma: **`[--key <chave de encriptação>]`** Pode, opcionalmente, colocar a chave de encriptação entre aspas duplas (").
Opção DHCP a utilizar	Opções de DHCP, delimitadas por vírgulas, utilizadas para recuperar perfis e firmware. O valor predefinido é 66,160,159,150,60,43,125.

Nome do parâmetro	Descrição e o valor predefinido
Mensagem de pedido de registo	Este parâmetro contém a mensagem enviada para o servidor syslog no início de uma tentativa de ressincronização. O valor predefinido é `$PN $MAC –A pedir % $SCHEME://$SERVIP:$PORT$PATH`.
Mensagem de sucesso de registo	A mensagem de syslog emitida após a conclusão bem-sucedida de uma tentativa de ressincronização. O valor predefinido é `$PN $MAC –Ressincronização bem sucedida % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Mensagem de falha de registo	A mensagem de syslog emitida após uma tentativa falhada de ressincronização. O valor predefinido é `$PN $MAC -- Ressincronização falhada: $ERR`.
Ressincronização configurável pelo utilizador	Permite a um utilizador ressincronizar o telefone a partir do ecrã do telefone IP. O valor predefinido é Sim.

Parâmetros de atualização de firmware

A tabela que se segue define a função e utilização de cada parâmetro na secção **Atualização de firmware** do separador **Aprovisionamento**.

Nome do parâmetro	Descrição e o valor predefinido
Ativar atualização	Permite operações de atualização de firmware independentemente das ações de ressincronização. O valor predefinido é Sim.
Atraso de repetição após erro na atualização	O intervalo de repetição de atualização (em segundos) aplicado em caso de falha de atualização. O dispositivo tem um temporizador de erros de atualização que ativa após uma tentativa falhada de atualização de firmware. O temporizador é inicializado com o valor neste parâmetro. A próxima tentativa de atualização de firmware ocorre quando a contagem deste temporizador chegar a zero. O valor predefinido é de 3600 segundos.

Nome do parâmetro	Descrição e o valor predefinido
Regra de atualização	Um script de atualização do firmware que define as condições de atualização URLs de firmware associados. Utiliza a mesma sintaxe que a Regra de perfil. Utilize o seguinte formato para introduzir a regra de atualização: **<tftp|http|https>://<endereço ip>/image/<nome de carga>** Por exemplo: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Se não for especificado um protocolo, é utilizado por predefinição TFTP. Se não for especificado um nome de servidor, o anfitrião que pede o URL é utilizado como nome do servidor. Se não for especificada uma porta, é utilizada a porta predefinida (69 para TFTP, 80 para HTTP ou 443 para HTTPS). O valor predefinido é em branco.
Mensagem de registo do pedido de atualização	Mensagem de syslog emitida no início de uma tentativa de atualização de firmware. Predefinição: `$PN $MAC -- Pedido de atualização $SCHEME://$SERVIP:$PORT$PATH`
Mensagem de registo de sucesso da atualização	Mensagem de syslog emitida após uma tentativa de atualização do firmware concluída com êxito. O valor predefinido é `$PN $MAC -- Atualização com sucesso $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Mensagem de registo de falha da atualização	Mensagem de syslog emitida após uma tentativa de atualização do firmware falhada. O valor predefinido é `$PN $MAC -- Atualização falhada: $ERR`
Partilhar firmware par a par	Ativa ou desativa a funcionalidade de partilha de firmware par a par. Selecione **Sim** ou **Não** para ativar ou desativar a funcionalidade. Predefinição: Sim
Servidor de registo de partilha de firmware par a par	Indica o endereço IP e a porta para os quais a mensagem UDP é enviada. Por exemplo: 10.98.76.123:514, em que 10.98.76.123 é o endereço IP e 514 é o número da porta.

Parâmetros genéricos

A tabela que se segue define a função e utilização de cada parâmetro na secção **Parâmetros genéricos** do separador **Aprovisionamento**.

Nome do parâmetro	Descrição e o valor predefinido
GPP A - GPP P	Os parâmetros genéricos GPP_* são utilizados como registos de cadeia de caracteres livre ao configurar os telefones para interagir com uma solução de servidor de aprovisionamento específico. Podem ser configurados para conter valores diversos, incluindo os seguintes: • Chaves de encriptação. • URLs. • Várias fases de informações de estado de aprovisionamento. • Modelos de pedido POST. • Mapas alias de nome do parâmetro. • Valores de cadeia de caracteres parciais, eventualmente combinados em valores de parâmetros completos. O valor predefinido é em branco.

Variáveis de expansão via macro

Determinadas variáveis de macro são reconhecidas dentro os seguintes parâmetros de aprovisionamento:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (em condições específicas)

Dentro destes parâmetros, certos tipos de sintaxe, como $NAME ou $(NAME), são reconhecidos e expandidos.

É possível especificar subcadeias de caracteres variáveis macro com a configuração $(NAME:p) e $(NAME:p:q), em que p e q são inteiros não negativos (disponível na revisão 2.0.11 e mais recentes). A expansão via macro resultante é subcadeia de caracteres que começa com o deslocamento de carácter p, com

comprimento q (ou até ao final da cadeia se q não for especificado). Por exemplo, se GPP_A contiver ABCDEF, então $(A:2) expande para CDEF, e $(A:2:3) expande para CDE.

Um nome não reconhecido não é traduzido e a forma $NAME ou $(NAME) permanece inalterada no valor do parâmetro após a expansão.

Nome do parâmetro	Descrição e o valor predefinido
$	A forma $$ expande para um único carácter $.
A a P	Substituído pelo conteúdo dos parâmetros genéricos GPP_A a GPP_P.
SA a SD	Substituído por parâmetros específicos GPP_SA a GPP_SD. Estes parâmetros contêm chaves ou palavras-passe utilizadas no aprovisionamento. **Nota** $SA a $SD são reconhecidos como argumentos para o qualificador de URL de ressincronização opcional, --key.
MA	Endereço MAC com dígitos hexadecimais minúsculos, por exemplo, 000e08aabbcc.
MAU	Endereço MAC com dígitos hexadecimais maiúsculos, por exemplo 000E08AABBCC.
MAC	Endereço MAC com dígitos hexadecimais minúsculos e vírgulas para separar pares de dígitos hexadecimais. Por exemplo, 00:0e:08:aa:bb:cc.
PN	Nome do produto. Por exemplo, CP-6841-3PCC.
PSN	Número de série do produto. Por exemplo, 6841-3PCC.
SN	Cadeia de caracteres do número de série. Por exemplo, 88012BA01234.
CCERT	Estado de certificado de cliente SSL: instalado ou não instalado.
IP	Endereço IP do telefone na respetiva sub-rede local. Por exemplo, 192.168.1.100.
EXTIP	IP externo do telefone, conforme visto na Internet. Por exemplo, 66.43.16.52.
SWVER	Cadeia de caracteres de versão do software. Por exemplo, sip68xx.11-0-1MPP.
HWVER	Cadeia de caracteres de versão do hardware. Por exemplo, 2.0.1

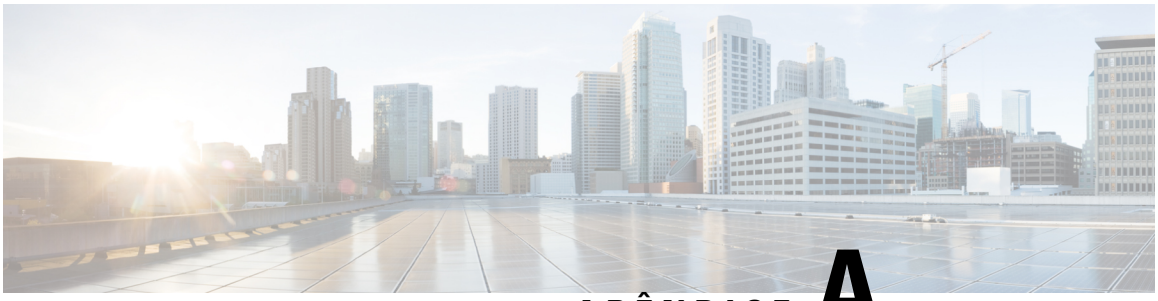
Nome do parâmetro	Descrição e o valor predefinido
PRVST	Estado de aprovisionamento (uma cadeia de caracteres numéricos): -1 = pedido explícito de ressincronização 0 = ressincronização ao ligar 1 = ressincronização periódica 2 = falha na ressincronização, tentativa de repetição
UPGST	Estado de atualização (uma cadeia de caracteres numérica): 1 = primeira tentativa de atualização 2 = falha na atualização, tentativa de repetição
UPGERR	Mensagem de resultado (ERR) da tentativa de atualização anterior; Por exemplo, falha de http_get.
PRVTMR	Segundos desde a última tentativa de ressincronização.
UPGTMR	Segundos desde a última tentativa de atualização.
REGTMR1	Segundos desde que a Linha 1 perdeu o registo com o servidor SIP.
REGTMR2	Segundos desde que a Linha 2 perdeu o registo com o servidor SIP.
UPGCOND	Nome de legado da macro.
SCHEME	Esquema de acesso ao ficheiro, TFTP, HTTP ou HTTPS, conforme obtido após a análise do URL de ressincronização ou atualização.
SERV	Pedido de nome de anfitrião do servidor de destino, conforme obtido após a análise do URL ressincronização ou atualização.
SERVIP	Pedido de endereço IP do servidor de destino, conforme obtido após a análise do URL de ressincronização ou atualização, possivelmente após pesquisa DNS.
PORT	Pedido de porta TCP/UDP de destino, conforme obtido após a análise do URL de ressincronização ou atualização.
PATH	Pedido de caminho de ficheiro de destino, conforme obtido após a análise do URL de ressincronização ou atualização.

Nome do parâmetro	Descrição e o valor predefinido
ERR	Mensagem de resultado da tentativa de ressincronização ou atualização. Útil apenas para geração de mensagens de resultado do syslog. O valor é preservado na variável UPGERR no caso de tentativas de atualização.
UIDn	O conteúdo do parâmetro de configuração UserID da linha n.
EMS	Estado Extension Mobility
MUID	Id do utilizador de Extension Mobility
MPWD	Palavra-passe de Extension Mobility

Códigos de erro interno

O telefone define um número de códigos de erro interno (X00 – X99) para facilitar a configuração fornecendo mais controlo sobre o comportamento da unidade em certas condições de erro.

Nome do parâmetro	Descrição e o valor predefinido
X00	Erro da camada de transporte (ou ICMP) erro ao enviar um pedido SIP.
X20	Pedido SIP expira enquanto aguarda uma resposta.
X40	Erro de protocolo SIP geral (por exemplo, codec inaceitável no SDP em mensagens ACK e 200, ou expira enquanto aguarda por ACK).
X60	Número marcado inválido segundo o plano de marcação acordado.



APÊNDICE A

Exemplos de perfis de configuração

Exemplo de formato aberto 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>
```

Exemplos de perfis de configuração

```
<!--  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  -->
 <!--  Wi-Fi Profile 1  -->
 <!--  Wi-Fi Profile 2  -->
 <!--  Wi-Fi Profile 3  -->
 <!--  Wi-Fi Profile 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>
<!--
 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>
```

Exemplos de perfis de configuração

```
<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 -- $ERR
</Log_Upgrade_Success_Msg>
<Log_Upgrade_Failure_Msg ua="na">$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>
```

Exemplos de perfis de configuração

```
<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)  -->
<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>
```

Exemplos de perfis de configuração

```
<!--
 available options:
e#20|e#1.0|e#10|e#90|e#80|e#70|e#60|e#50|e#40|e#30|e#20|e#10|e#1.0|e#20|e#30|e#40|e#50|e#5|e#60|e#80|e#70|e#80|e#90|e#98|e#10|e#1.0|e#20|e#30|e#40

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

Exemplos de perfis de configuração

```
<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  -->
<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
```

Exemplos de perfis de configuração

```
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_>
```

Exemplos de perfis de configuração

```
<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_>
<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_>
```

Exemplos de perfis de configuração

```
<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  -->
<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_>
```

Exemplos de perfis de configuração

```
<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_>
<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
-->
```

Exemplos de perfis de configuração

```
<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"/>
 <!--  <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"/>
```

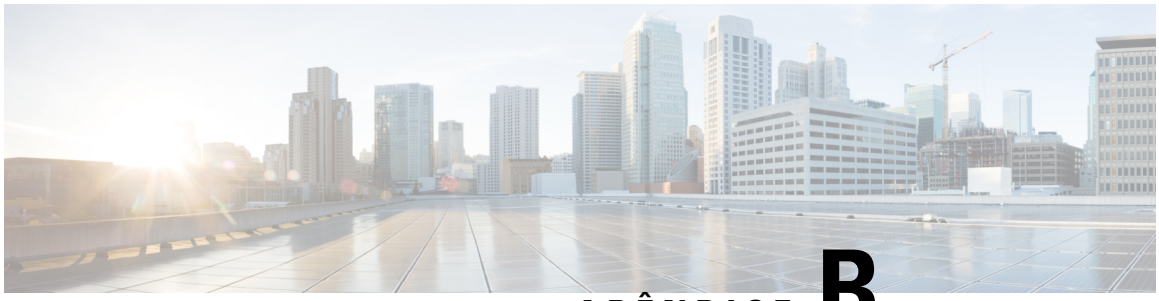
Exemplos de perfis de configuração

```
<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"/>
```

Exemplos de perfis de configuração

```
 <!--  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>
```



APÊNDICE B

Acrónimos

Acrónimos

CA	Corrente alternada
ACS	Servidor de Controlo de Acesso
A/D	Conversor analógico para digital
AES	Padrão de encriptação avançada
ANC	Chamada anónima
AP	Ponto de Acesso (AP)
ASCII	American Standard Code for Information Interchange
B2BUA	Agente de utilizador back-to-back
BLF	Definições BLF (Busy Lamp Field)
Bool	Valores booleanos. Especificado como sim e não, ou 1 e 0 no perfil
BootP	Protocolo Bootstrap
CA	Autoridade de certificação
CAS	Sinal de alerta do CPE
CDP	Cisco Discovery Protocol
CDR	Registo dos detalhes da chamada
CGI	Imagens geradas por computador
CID	ID do chamador
CIDCW	ID do chamador da chamada em espera

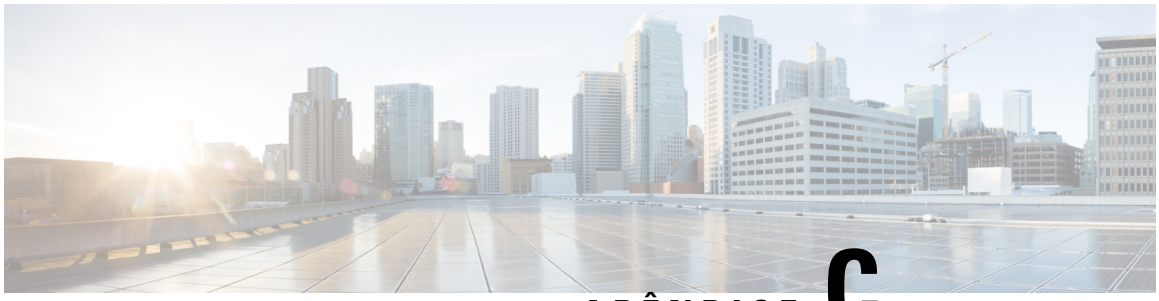
CNG	Geração de ruído confortável
CPC	Controlo de autor da chamada
CPE	Equipamento das instalações do cliente
CSV	Valor separado por vírgulas
CWCID	ID do chamador da chamada em espera
CWT	Tom de chamada em espera
D/A	Conversor digital para analógico
dB	decibel
dBm	dB relativamente a 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
DND	Não interromper
DNS	Sistema de nome do domínio
DoS	Negação de serviço
DRAM	Memória de acesso aleatório dinâmico
DSL	Loop de subscritor digital
DSP	Processador de sinal digital
DST	Horário de verão
DTAS	Sinal de alerta do terminal de dados (igual a CAS)
DTMF	Dual Tone Multiple Frequency
FQDN	Nome de domínio totalmente qualificado
FSK	Criação de chaves para troca de frequência
FW	Firmware
FXS	Estação de intercâmbio
GMT	Hora do meridiano de Greenwich
GW	Gateway
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP sobre SSL
ICMP	Internet Control Message Protocol

IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	Protocolo de Internet versão 4
IPv6	Protocolo de Internet versão 6
ISP	Provedor de serviços de Internet
ITSP	Provedor de serviços de telefonia por Internet
ITU	União internacional de telecomunicações
IVR	Resposta de voz interactiva
LAN	Rede local
LBR	Velocidade de transmissão baixa
LBRC	Codec de velocidade de transmissão baixa
LCD	Ecrã de cristais líquidos; também conhecido por ecrã
LDAP	Lightweight Directory Access Protocol
LED	Díodo emissor de luz
Endereço MAC	Endereço Media Access Control
MC	Mini-certificado
MGCP	Media Gateway Control Protocol
MOH	Music On Hold
MOS	Pontuação média de opinião (1-5, quanto mais alto melhor)
MPP	Telefones multiplataforma
ms	Milissegundo
MSA	Music Source Adaptor
MWI	Indicação de mensagem em espera
NAT	Tradução de endereço de rede
(NPS)	Servidor de aprovisionamento normal
NTP	Protocolo de hora da rede
OOB	Fora de banda

OSI	Abrir intervalo de comutação
PBX	Central telefónica privada
PCB	Placa de circuitos impressos
PoE	Power over Ethernet
RP	Inversão de polaridade
PS	Servidor de aprovisionamento
PSQM	Medição de qualidade de perceção do discurso (1-5, quanto mais baixo melhor)
PSTN	Rede telefónica pública comutada
QoS	Qualidade do serviço
RC	Remover personalização
REQT	(SIP) Mensagem de pedido
RESP	(SIP) Mensagem de resposta
RSC	(SIP) Código de estado de resposta, como 404, 302, 600
RTP	Real Time Protocol
RTT	Tempo de ida e volta
SAS	Servidor de transmissão de áudio
SDP	Session Description Protocol
SDRAM	DRAM síncrona
seg	segundos
SIP	Protocolo de inicialização da sessão
SLA	Aspeto da linha partilhada
SLIC	Circuito de interface de linha de assinante
SP	Fornecedor de serviços
SSL	Secure Socket Layer
STUN	Session Traversal UDP for NAT
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTL	Time to live

ToS	Tipo de serviço
UA	Agente de utilizador
uC	Micro-controlador
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VAR	Revendedor de valor acrescentado
VLAN	LAN de voz
VM	Correio de voz
VMWI	Indicação/indicador visual de mensagem em espera
VoIP	Protocolo de voz sobre a Internet
VQ	Qualid. da voz
WAN	Rede alargada
XML	Extensible Markup Language

Acrónimos



APÊNDICE C

Documentação relacionada

Documentação relacionada

Utilize as secções seguintes para obter informações relacionadas.

Documentação do telefone Cisco IP Phone série 6800

Consulte publicações específicas do seu idioma, modelo de telefone e versão de firmware multiplataforma. Navegue a partir do seguinte Uniform Resource Locator (URL):

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

Política de suporte de firmware do Cisco IP Phone

Para obter informações sobre a política de suporte para telefones, consulte https://cisco.com/go/phonefirmwaresupport.