Guía de aprovisionamiento de los teléfonos multiplataforma para Cisco IP Phone serie 6800

Primera publicación: 2017-11-22

Última modificación: 2019-08-05

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONTENIDO

CAPÍTULO 1

Implementación y aprovisionamiento

Información nueva y modificada

Funciones nuevas y modificadas para la versión de firmware 11.2(4)

Revisión	Secciones nuevas y modificadas
Parámetros agregados para la configuración de Wi-Fi	Ejemplo de formato abierto XML, en la página 83

Funciones nuevas y modificadas para la versión de firmware 11.2(3)SR1

Las siguientes secciones son novedades o se han actualizado para la compatibilidad con Teléfonos multiplataforma Cisco IP Phone 6800 Series.

Revisiones	Secciones nuevas y modificadas
Se ha agregado un tema nuevo para presentar la incorporación del código de activación.	Incorporación del teléfono con el código de activación , en la página 11

Funciones nuevas y modificadas para la versión de firmware 11.2(3)

Las siguientes secciones son novedades o se han actualizado para la compatibilidad con Teléfonos multiplataforma Cisco IP Phone 6800 Series.

Revisiones	Secciones nuevas y modificadas
Se ha agregado un tema de concepto para el cifrado de perfil abierto.	Cifrado de perfil abierto, en la página 20
Se ha agregado un nuevo tema para introducir el cifrado de contenido HTTP basado en RFC 8188.	Cifrado de contenido de HTTP basado en RFC 8188, en la página 25
Se ha actualizado con información sobre el cifrado basado en RFC 8188.	Formatos de perfil de configuración, en la página 15 Aprovisionamiento de HTTP, en la página 45
Se han actualizado los detalles de fábrica para el cifrado de perfil abierto.	Cifrado AES-256-CBC, en la página 21
Se ha actualizado la descripción de la opción **`--clave`** y se ha agregado una nota acerca del cifrado basado en RFC 8188.	key, en la página 25 Parámetros de perfil de configuración, en la página 71
Se han actualizado los ejemplos de formato abierto XML con nuevos parámetros y opciones disponibles	Ejemplo de formato abierto XML, en la página 83

Funciones nuevas y modificadas para la versión de firmware 11.2(1)

Revisiones	Secciones nuevas o modificadas
Se ha actualizado el tema con una referencia a la comparación de los parámetros XML y TR69	Aprovisionamiento de TR69, en la página 4
Se ha agregado un nuevo tema para la compatibilidad con la características de encabezado de privacidad	Configurar el encabezado de privacidad del teléfono, en la página 70
Se ha agregado un nuevo tema para compartir el firmware en el grupo	Uso compartido del firmware en el grupo, en la página 12
Se ha actualizado este tema con los métodos de cifrado	Obtención de un certificado de servidor firmado, en la página 48
Se ha actualizado este tema para compatibilidad con la característica de omisión de la pantalla de **Configuración de la contraseña**	Control de acceso de configuración, en la página 9
Se ha agregado un nuevo tema para la compatibilidad con la omisión de la pantalla **Configuración de la contraseña**	Omitir la pantalla de configuración de contraseña, en la página 13

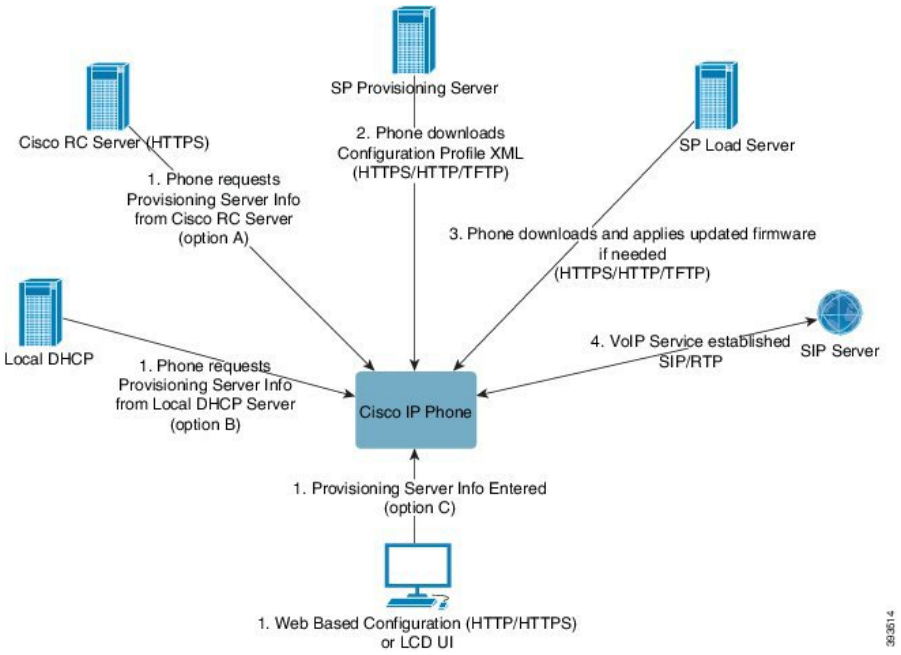
Información general sobre el aprovisionamiento

Los teléfonos Cisco IP Phone se han diseñado para implementaciones de gran volumen por proveedores de servicios de voz sobre IP (VoIP) para clientes en entornos domésticos, de negocios o empresariales. El aprovisionamiento del teléfono mediante la administración y la configuración remota garantiza el funcionamiento correcto del teléfono en el emplazamiento del cliente.

Cisco es compatible con la configuración personalizada de funciones del teléfono utilizando lo siguiente:

- Control remoto fiable del teléfono.
- Cifrado de la comunicación que controla el teléfono.
- Enlace de cuenta de teléfono optimizado.

Los teléfonos se pueden suministrar para descargar perfiles de configuración o firmware actualizado de un servidor remoto. Las descargas se realizan cuando los teléfonos están conectados a una red, cuando están encendidos y a intervalos establecidos. El aprovisionamiento suele formar parte de implementaciones de gran volumen de VoIP comunes por parte de los proveedores de servicios. Los perfiles de configuración o el firmware actualizado se transfieren al dispositivo mediante TFTP, HTTP o HTTPS.



En un alto nivel, el proceso de aprovisionamiento del teléfono es el siguiente:

1. Si el teléfono no está configurado, la información del servidor de aprovisionamiento se aplica al teléfono mediante una de las siguientes opciones:
   - **A**: se descarga desde el servidor de personalización remota (RC) del sistema Cisco Enablement Data Orchestration System (EDOS) mediante HTTPS.
   - **B**: se consulta desde un servidor DHCP local.
   - **C**: se introduce manualmente a través de la utilidad de configuración basada en web del teléfono Cisco o la interfaz de usuario del teléfono.

2. El teléfono descarga la información del servidor de aprovisionamiento y aplica la configuración XML mediante el protocolo HTTPS, HTTP o TFTP.
3. El teléfono descarga y aplica el firmware actualizado, si fuera necesario, a través de HTTPS, HTTP o TFTP.
4. El servicio VoIP se establece mediante la configuración y el firmware especificados.

Los proveedores de servicios de VoIP pretenden implementar un gran volumen de teléfonos para los clientes residenciales y las pequeñas empresas. En entornos de negocios o empresariales, los teléfonos pueden servir como nodos terminales. Estos servicios, que están conectados a través de routers y cortafuegos en instalaciones de los clientes, se distribuyen ampliamente en Internet.

El teléfono puede utilizarse como una extensión remota del equipo back-end del proveedor de servicio. La administración y la configuración remota garantizan el buen funcionamiento del teléfono en las instalaciones del cliente.

Aprovisionamiento de TR69

El Cisco IP Phone ayuda al administrador a configurar los parámetros de TR69 mediante la interfaz de usuario Web. Para obtener información relacionada con los parámetros, incluyendo una comparación de los parámetros XML y TR69, consulte la Guía de administración para la serie del teléfono correspondiente.

Los teléfonos admiten la detección automática de servidores de configuración (ACS) mediante DHCP, opción 43, 60 y 125.

- Opción 43: información específica del proveedor para la URL de ACS.
- Opción 60: identificador de clase de proveedor, el teléfono se identifica con `dslforum.org` a ACS.
- Opción 125: información específica del proveedor para la asociación a la puerta de enlace.

Métodos RPC

Métodos RPC admitidos

Los teléfonos solo admiten un conjunto limitado de métodos de llamada de procedimientos remotos (RPC), como se indica a continuación:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject

- Reboot
- FactoryReset
- Inform
- Download: método de descarga RPC, los tipos de archivo compatibles son:
  - Imagen de actualización de firmware
  - Archivo de configuración del proveedor
  - Archivo de entidad emisora de certificados (CA, Certificate Authority) personalizado
- Transferencia completa

Tipos de evento compatibles

Los teléfonos permiten tipos de eventos basados en funciones y métodos compatibles. Solo se admiten los siguientes tipos de eventos:

- Bootstrap
- Arranque
- Cambio de valor
- Solicitud de conexión
- Periódico
- Transferencia completa
- Descarga de M
- Reinicio de M

Cifrado de comunicación

Los parámetros de configuración que se comunican con el dispositivo pueden contener códigos de autorización u otra información que protege el sistema de acceso no autorizado. Es de interés del proveedor de servicios para evitar la actividad del cliente no autorizado. Es de interés del cliente para evitar el uso no autorizado de la cuenta. El proveedor de servicios puede cifrar la comunicación del perfil de configuración entre el servidor de aprovisionamiento y el dispositivo, además de restringir el acceso al servidor web de administración.

Comportamiento del teléfono durante horas de congestión de red

Cualquier circunstancia que degrade el rendimiento de la red puede afectar a la voz y, en algunos casos, puede provocar que una llamada se interrumpa. Algunas actividades, entre otras, que degradan la red pueden ser:

- Las tareas administrativas, como la exploración de puertos internos o las exploraciones de seguridad.

- Los ataques que pueda recibir la red, como ataques de denegación de servicio.

Implementación

Los Cisco IP Phone proporcionan mecanismos adecuados para el aprovisionamiento, en función de los modelos de implementación:

- Distribución de forma masiva: el proveedor de servicios adquiere los Cisco IP Phone en grandes cantidades y realiza el aprovisionamiento previo internamente o compra unidades de personalización remota (RC) de Cisco. A continuación, los dispositivos se emiten a los clientes como parte de un contrato de servicio de VoIP.
- Distribución minorista: el cliente compra el Cisco IP Phone de un minorista y solicita un servicio VoIP del proveedor de servicios. A continuación, el proveedor de servicios debe admitir la configuración segura remota del dispositivo.

Distribución de forma masiva

En este modelo, el proveedor de servicios proporciona los teléfonos a sus clientes como parte de un contrato de servicio de VoIP. Los dispositivos son unidades RC o se aprovisionan previamente de forma interna.

Cisco aprovisiona previamente las unidades RC para resincronizar con un servidor de Cisco que descarga las actualizaciones de firmware y del perfil de dispositivo.

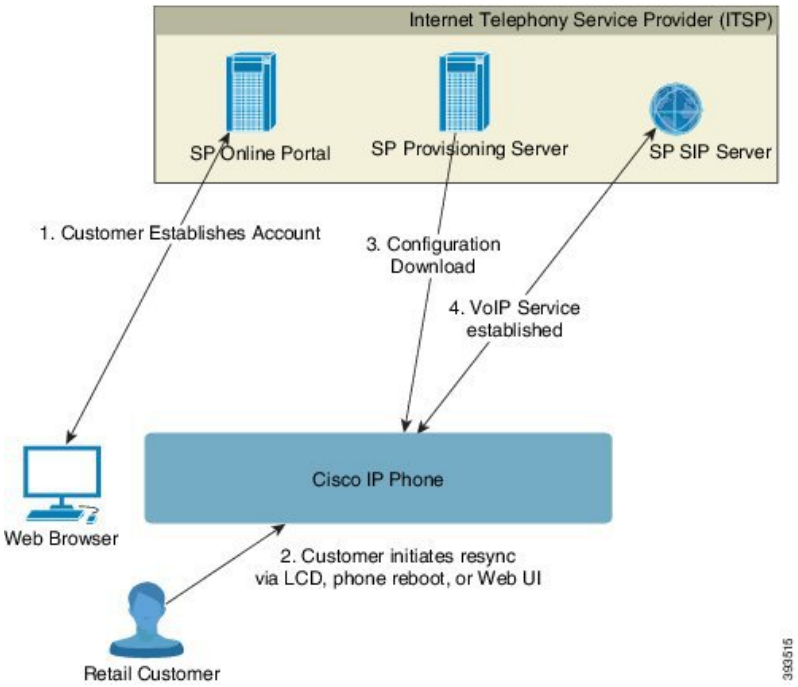
Un proveedor de servicios puede aprovisionar previamente los teléfonos con los parámetros deseados, incluidos los parámetros que controlan la resincronización, a través de varios métodos:

- Internamente mediante DHCP y TFTP
- De forma remota mediante TFTP, HTTP o HTTPS
- Una combinación de aprovisionamiento interno y remoto

Distribución comercial

En un modelo de distribución comercial, un cliente adquiere un teléfono y se suscribe a un servicio específico. El proveedor de servicio de telefonía de Internet (ITSP) configura y mantiene un servidor de aprovisionamiento y realiza el aprovisionamiento previo del teléfono para resincronizarse con el servidor del proveedor de servicio.

Figura 1: Distribución comercial



El teléfono incluye la utilidad de configuración basada en web que muestra la configuración interna y acepta valores de parámetro de configuración nuevos. El servidor también acepta una sintaxis de comandos de URL especial para realizar operaciones de actualización de firmware y de resincronización del perfil remoto.

El cliente inicia sesión en el servicio y establece una cuenta de VoIP, posiblemente a través de un portal en línea y enlaza el dispositivo a la cuenta de servicio asignada. Se indica al teléfono sin aprovisionar que se resincronice con un servidor de aprovisionamiento específico a través de un comando de URL de resincronización. El comando de URL normalmente incluye una cuenta con el número de ID de cliente o un código alfanumérico para asociar el dispositivo con la nueva cuenta.

En el ejemplo siguiente, se indica a un dispositivo en la dirección IP asignada por DHCP 192.168.1.102 que se aprovisione el propio al servicio SuperVoIP:

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

En este ejemplo, 1234abcd es el número de ID de cliente de la nueva cuenta. El servidor de aprovisionamiento remoto asocia el teléfono que realiza la solicitud de resincronización con la nueva cuenta, en función de la dirección URL y el ID de cliente proporcionado. A través de esta operación de resincronización inicial, el teléfono se configura en un solo paso. Se indicará automáticamente al teléfono que se resincronice posteriormente con una dirección URL permanente del servidor. Por ejemplo:

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

Para el acceso inicial y permanente, el servidor de aprovisionamiento se basa en el certificado del cliente del teléfono para la autenticación. El servidor de aprovisionamiento proporciona valores del parámetro de configuración correctos en función de la cuenta de servicio asociada.

Cuando el dispositivo está encendido o ha transcurrido el tiempo especificado, el teléfono se resincroniza y descarga los parámetros más recientes. Estos parámetros pueden lograr objetivos tales como establecer un grupo de salto, establecer números de marcación rápida de configuración y limitar las funciones que un usuario puede modificar.

Temas relacionados

Aprovisionamiento previo de un dispositivo interno, en la página 44

Proceso de resincronización

El firmware para cada teléfono incluye un servidor de administración web que acepta los nuevos valores de parámetro de configuración. Puede indicar al teléfono que resincronice la configuración tras el reinicio o a intervalos programados con un servidor de aprovisionamiento específico mediante un comando de URL de resincronización del perfil del dispositivo.

De forma predeterminada, el servidor web está activado. Para desactivar o activar el servidor web, utilice el comando de la URL de resincronización.

Si fuera necesario, podrá solicitar una resincronización inmediata a través de una URL de acción de "resincronización". El comando de la URL de resincronización puede incluir un número de ID de cliente de cuenta o un código alfanumérico para asociar de forma exclusiva el dispositivo con la cuenta del usuario.

Ejemplo

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

En este ejemplo, se indica a un dispositivo en la dirección IP asignada por DHCP 192.168.1.102 que se aprovisione el propio al servicio SuperVoIP en prov.supervoip.com. El número de ID de cliente para la nueva cuenta es 1234abcd. El servidor de aprovisionamiento remoto asocia el teléfono que realiza la solicitud de resincronización con la nueva cuenta, en función de la dirección URL y el ID de cliente.

A través de esta operación de resincronización inicial, el teléfono se configura en un solo paso. Se indicará automáticamente al teléfono que se resincronice posteriormente con una dirección URL permanente del servidor.

Para el acceso inicial y permanente, el servidor de aprovisionamiento se basa en el certificado del cliente para la autenticación. El servidor proporciona valores del parámetro de configuración en función de la cuenta de servicio asociada.

Aprovisionamiento

Un teléfono se puede configurar para resincronizar su estado interno de forma que concuerde con un perfil remoto periódicamente y durante el encendido. El teléfono se pone en contacto con un servidor de aprovisionamiento normal (NPS) o un servidor de control de acceso (ACS).

De forma predeterminada, un perfil de resincronización solo se intenta cuando el teléfono está inactivo. Esta práctica impide una actualización que desencadenaría un reinicio del software e interrumpiría una llamada. Si se necesitan actualizaciones intermedias para alcanzar un estado actual de actualización desde una versión anterior, la lógica de actualización puede automatizar actualizaciones multifase.

Servidor de aprovisionamiento normal

El servidor de aprovisionamiento Normal (NPS) puede ser un servidor TFTP, HTTP o HTTPS. Se logra una actualización de firmware remota mediante TFTP o HTTP o HTTPS, porque el firmware no contiene información confidencial.

Aunque se recomienda HTTPS, la comunicación con NPS no requiere el uso de un protocolo seguro porque el perfil actualizado se puede cifrar mediante una clave secreta compartida. Para obtener más información acerca de la utilización de HTTPS, consulte Cifrado de comunicación, en la página 5. Se proporciona un aprovisionamiento por primera vez mediante un mecanismo que utiliza la funcionalidad SSL. Un teléfono no aprovisionado puede recibir un perfil cifrado con una clave simétrica de 256 bits diseñada para ese dispositivo.

Control de acceso de configuración

El firmware del teléfono proporciona mecanismos para restringir el acceso del usuario final a algunos parámetros. El firmware proporciona privilegios específicos para iniciar sesión en una cuenta de **Admin** o una cuenta de **Usuario**. Cada una se puede proteger independientemente mediante una contraseña.

- Cuenta de administrador: otorga al proveedor de servicios acceso completo a todos los parámetros del servidor web de administración.
- Cuenta de usuario: permite al usuario configurar un subconjunto de parámetros del servidor web de administración.

El proveedor de servicios puede restringir la cuenta de usuario en el perfil de aprovisionamiento de las formas siguientes:

- Indicar los parámetros de configuración que se encuentran disponibles en la cuenta de usuario al crear la configuración.
- Desactivar el acceso del usuario al servidor web de administración.
- Desactivar el acceso de usuario para la interfaz de usuario de la pantalla LCD.
- Omitir la pantalla de **Configuración de la contraseña** para el usuario.
- Restringir los dominios de Internet a los que el dispositivo accede para la resincronización, las actualizaciones o el registro SIP para la Línea 1.

Temas relacionados

Propiedades de la etiqueta de elemento, en la página 16
Control de acceso, en la página 18

Acceso a la página web del teléfono

Si el proveedor de servicios ha desactivado el acceso a la utilidad de configuración, póngase en contacto con él antes de continuar.

Procedimiento

Paso 1 Asegúrese de que el ordenador se puede comunicar con el teléfono. No debe haber ninguna VPN en uso.

Paso 2 Inicie un explorador web.

Paso 3 Introduzca la dirección IP del teléfono en la barra de dirección del navegador.

- Acceso de usuario: **http://<dirección ip>/**
- Acceso de administrador: **http://<dirección ip>/admin/advanced**
- Acceso de administrador: **http://<dirección ip>**, haga clic en **Inicio de sesión de Admin** y haga clic en **Avanzado**

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

Paso 4 Introduzca la contraseña cuando se le solicite.

Permiso de acceso a web del Cisco IP Phone

Para ver los parámetros del teléfono, active el perfil de configuración. Para efectuar cambios en cualquiera de los parámetros, debe poder cambiar el perfil de configuración. Puede que el administrador del sistema haya desactivado la opción del teléfono para permitir que la interfaz del usuario web del teléfono se pueda ver o se pueda escribir en ella.

Para obtener más información, consulte la *Guía de aprovisionamiento de teléfonos multiplataforma Cisco IP Phone 6800 Series*.

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Haga clic en **Voz** > **Sistema**.

Paso 2 En la sección **Configuración del sistema**, en **Activar servidor web** establezca el valor **Sí**.

Paso 3 Para actualizar el perfil de configuración, haga clic en **Enviar todos los cambios** después de modificar los cambios en la interfaz del usuario web del teléfono.

El teléfono se inicia y los cambios se aplican.

Paso 4 Para borrar todos los cambios que ha realizado durante la sesión actual (o tras la última vez que hizo clic en **Enviar todos los cambios**), haga clic en **Deshacer todos los cambios**. Los ajustes vuelven a los valores anteriores.

Medidas de aprovisionamiento del teléfono

Por lo general, el Cisco IP Phone está configurado para el aprovisionamiento la primera vez que se conecta a la red. El teléfono también se aprovisiona en los intervalos programados cuando el proveedor de servicios o el VAR realiza el aprovisionamiento previo (configuración) del teléfono. Los proveedores de servicios pueden autorizar a los VAR o a los usuarios avanzados a aprovisionar manualmente el teléfono mediante el teclado del teléfono. Usted también puede configurar el aprovisionamiento mediante la interfaz de usuario web del teléfono.

Marque **Estado** > **Estado del teléfono** > **Aprovisionamiento** en la interfaz de usuario de la pantalla LCD del teléfono o el estado de aprovisionamiento en la ficha **Estado** de la utilidad de configuración web.

Temas relacionados

Aprovisionar manualmente un teléfono desde el teclado, en la página 11

Incorporación del teléfono con el código de activación

Esta función está disponible en la versión de firmware 11-2-3MSR1, BroadWorks Application Server Release 22.0 (parche AP.as.22.0.1123.ap368163 y sus dependencias). Sin embargo, puede cambiar los teléfonos con un firmware antiguo para utilizar esa función. Puede indicar al teléfono que actualice al nuevo firmware y que utilice la regla de perfil `gds://` para activar la pantalla de código de activación. Un usuario introduce un código de 16 dígitos en el campo proporcionado para que el teléfono se incorpore automáticamente.

Nota El Teléfonos multiplataforma Cisco IP Phone 6861 no admite el código de activación incorporado.

Antes de empezar

Asegúrese de que permite que el servicio activation.webex.com a través del firewall admita la incorporación mediante el código de activación.

Procedimiento

Paso 1 Edite el archivo config.xml en un editor de texto o XML.

Paso 2 Siga el ejemplo siguiente en el archivo config.xml para establecer la regla de perfil para la incorporación del código de activación.

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

Paso 3 Guarde los cambios en el archivo config.xml.

Aprovisionar manualmente un teléfono desde el teclado

Procedimiento

Paso 1 Pulse **Aplicaciones** .

Paso 2 Seleccione **Administración de dispositivos** > **Regla de perfil**.

Paso 3 Introduzca la regla de perfil mediante el siguiente formato:

```
protocolo://servidor[:puerto]/vía_del_perfil
```

Por ejemplo:

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

Si no se especifica ningún protocolo, se utiliza TFTP. Si no se especifica ningún nombre de servidor, se usa en su lugar el host que solicita la URL. Si no se especifica ningún puerto, se usa el predeterminado (69 para TFTP, 80 para HTTP o 443 para HTTPS).

Paso 4 Pulse **Resincronizar**.

Temas relacionados

Medidas de aprovisionamiento del teléfono, en la página 10

Uso compartido del firmware en el grupo

Compartir firmware en el grupo (PFS) es un modelo de distribución de firmware que permite a un Cisco IP Phone buscar otros teléfonos del mismo modelo o de la misma serie en la subred y compartir los archivos de firmware actualizados cuando se necesita actualizar varios teléfonos al mismo tiempo. PFS utiliza el protocolo CPPDP (Cisco Peer-to-Peer-Distribution Protocol), que es un protocolo propiedad de Cisco. Con CPPDP, todos los dispositivos de la subred forman una jerarquía punto a punto y, a continuación, copian el firmware o los otros archivos de dispositivos iguales a los dispositivos del entorno. Para optimizar las actualizaciones del firmware, un teléfono raíz descarga la imagen de firmware del servidor de subida y, a continuación, transfiere el firmware a otros teléfonos en la subred que usan conexiones TCP.

Uso compartido del firmware en el grupo:

- Limita la congestión de las transferencias TFTP a los servidores de subida remotos centralizados.
- Elimina la necesidad de controlar manualmente las actualización del firmware.
- Reduce el tiempo de inactividad del teléfono durante las actualizaciones cuando se restauran simultáneamente grandes cantidades de teléfonos.

Nota

- El uso compartido de firmware en el grupo no funcionará a menos que se configuren varios teléfonos para que se actualicen al mismo tiempo. Cuando se envía NOTIFY con Event:resync, se inicia una resincronización en el teléfono. Ejemplo de un xml que puede contener las configuraciones para iniciar la actualización:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Cuando configura el servidor de subida para compartir el firmware en el grupo a una dirección IP y un puerto, los registros específicos de PFS se envían a ese servidor como mensajes UDP. Este ajuste se debe realizar en cada teléfono. A continuación, puede utilizar los mensajes de registro para solucionar los problemas relacionados con PFS.

Peer_Firmware_Sharing_Log_Server especifica el nombre de host de servidor de registro de UDP remoto y el puerto. El puerto predeterminado es el puerto predeterminado 514 del registro del sistema.

Por ejemplo:

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

Para utilizar esta función, active PFS en los teléfonos.

Omitir la pantalla de configuración de contraseña

Puede omitir la pantalla de **Configuración de la contraseña** del teléfono en el primer arranque o tras un restablecimiento a los valores de fábrica en estas acciones de aprovisionamiento:

- Configuración de DHCP
- Configuración de EDOS
- Configuración de la contraseña del usuario mediante el archivo de configuración XML del teléfono.

Tabla 1: Acciones de aprovisionamiento que determinan si se muestra la pantalla de Configuración de la contraseña

DHCP configurado	EDOS configurado	Contraseña del usuario configurada	Omitir pantalla de configuración de contraseña
Sí	n/a	Sí	Sí
Sí	n/a	No	**No**
No	Sí	Sí	Sí
No	Sí	No	**No**
No	No	n/a	**No**

Procedimiento

Paso 1 Edite el archivo `cfg.xml` del teléfono en un texto o editor XML.

Paso 2 Inserte la etiqueta **<User_Password>** mediante unas de estas opciones.

- **Sin contraseña (etiqueta inicial y final)**–**<User_Password></User_Password>**
- **Valor de contraseña (de 4 a 127 caracteres)**–**<User_Password ua="rw">Abc123</User_Password>**
- **Sin contraseña (solo etiqueta inicial)**–**<User_Password />**

Paso 3 Guarde los cambios en el archivo `cfg.xml`.

La pantalla **Definir contraseña** no aparece cuando arranca por primera vez o después de un restablecimiento de los valores de fábrica. Si se especifica una contraseña, se le solicitará al usuario que la introduzca al acceder a la página web del teléfono o a los menús de la pantalla del teléfono.

CAPÍTULO 2

Formatos de aprovisionamiento

Secuencias de comandos de aprovisionamiento

El teléfono acepta la configuración en formato XML.

Para obtener información detallada sobre su teléfono, consulte la Guía de administración para el dispositivo en cuestión. Cada guía describe los parámetros que pueden configurarse a través del servidor web de administración.

Formatos de perfil de configuración

El perfil de configuración define los valores de los parámetros para el teléfono.

El formato del perfil de configuración XML utiliza herramientas de edición de XML estándar para compilar los parámetros y valores.

Nota Solo se admite el conjunto de caracteres UTF-8. Si modifica el perfil en un editor, no cambie el formato de codificación; de lo contrario, el teléfono no reconoce el archivo.

Cada modelo de teléfono tiene un conjunto de funciones diferentes y, por lo tanto, un conjunto de parámetros diferente.

Perfil de formato XML (XML)

El perfil de formato abierto es un archivo de texto con sintaxis XML en una jerarquía de elementos, con los atributos del elemento y los valores. Este formato le permite utilizar las herramientas estándar para crear el

archivo de configuración. Se puede enviar un archivo de configuración en este formato desde el servidor de aprovisionamiento al teléfono durante una operación de resincronización. Se puede enviar el archivo sin compilación como un objeto binario.

El teléfono puede aceptar los formatos de configuración que las herramientas estándar generan. Esta función facilita el desarrollo de software del servidor de aprovisionamiento back-end que genera los perfiles de configuración de bases de datos existentes.

Para proteger la información confidencial del perfil de configuración, el servidor de aprovisionamiento envía este tipo de archivo al teléfono mediante un canal protegido mediante TLS. De manera opcional, se puede comprimir el archivo utilizando el algoritmo deflación (RFC1951) de gzip.

El archivo se puede cifrar con uno de estos métodos de cifrado:

- Cifrado AES-256-CBC
- Cifrado de contenido HTTP basado en RFC-8188 con cifrado AES-128-GCM

Ejemplo: formato de perfil abierto

```
<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>
```

La etiqueta de elemento <flat-profile> incluye todos los elementos de parámetros que el teléfono reconoce.

Temas relacionados

Compresión y cifrado de perfil abierto (XML), en la página 20

Componentes del archivo de configuración

Un archivo de configuración puede incluir estos componentes:

- Etiquetas de elemento
- Atributos
- Parámetros
- Características de formato
- Comentarios XML

Propiedades de la etiqueta de elemento

- El archivo XML de aprovisionamiento de formato y la interfaz de usuario web permiten establecer la misma configuración. El nombre de la etiqueta XML y los nombres de campo de la interfaz de usuario web son similares pero varían debido a las restricciones de nombre de elemento XML. Por ejemplo, guiones bajos (_) en lugar de " ".

- El teléfono reconoce los elementos con los nombres de parámetro correctos que se encapsulan en el elemento especial <flat-profile>.
- Los nombres de los elementos se incluyen entre corchetes angulares.
- La mayoría de los nombres de los elementos son similares a los nombres de los campos de las páginas web de administración para el dispositivo, con las modificaciones siguientes:
  - Los nombres de los elementos no pueden incluir espacios ni caracteres especiales. Para derivar el nombre del elemento del nombre del campo de administración web, sustituya con un guion bajo cada espacio o los caracteres especiales `[`, `]`, `(`, `)` o `/`.

    Ejemplo: el elemento <Resync_On_Reset> representa el valor del campo **Resincronizar al restablecer**.
  - El nombre de cada elemento debe ser único. En las páginas web de administración, los mismos campos pueden aparecer en varias páginas web, como las páginas de línea, usuario y extensión. Adjunte `[n]` al nombre del elemento para indicar el número que se muestra en la ficha de la página.

    Ejemplo: el elemento <Dial_Plan_1_> representa el **Plan de marcación** para la línea 1.
- Cada etiqueta de elemento de apertura debe tener una coincidencia de etiqueta de elemento de cierre. Por ejemplo:

```
<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>
```

- Las etiquetas de elemento distinguen mayúsculas de minúsculas.
- Las etiquetas de elemento vacío se permiten y se interpretarán como configurar el valor de estar vacío. Introduzca la etiqueta de elemento de apertura sin una etiqueta de elemento correspondiente e inserte un espacio y una barra diagonal antes del corchete angular de cierre (>). En este ejemplo, la regla de perfil B está vacía:

```
<Profile_Rule_B />
```

- Se puede usar una etiqueta de elemento vacía para evitar la sobrescritura de cualquier valor proporcionado por el usuario durante una operación de resincronización. En el siguiente ejemplo, los ajustes de marcación rápida de usuario se dejan sin modificar:

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

```
<Speed_Dial_8_Name ua="rw"/>
<Speed_Dial_8_Number ua="rw"/>
<Speed_Dial_9_Name ua="rw"/>
<Speed_Dial_9_Number ua="rw"/>
</flat-profile>
```

- Utilice un valor vacío para establecer el parámetro correspondiente a una cadena vacía. Introduzca un elemento de apertura y cierre sin ningún valor entre ellos. En el ejemplo siguiente, se establece el parámetro GPP_A en una cadena vacía.

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

- Se ignorarán los nombres de los elementos no reconocidos.

Temas relacionados

Control de acceso de configuración, en la página 9

Atributo de acceso de usuario

Se pueden usar los controles de atributo de acceso de usuario (**ua**) para cambiar el acceso mediante la cuenta de usuario. Si no se especifica el atributo **ua**, se conserva la configuración de acceso de usuario existente. Este atributo no afecta al acceso por parte de la cuenta de administrador.

Si está presente, el atributo **ua** debe tener uno de los siguientes valores:

- na: sin acceso
- ro: solo lectura
- rw: lectura y escritura

En el ejemplo siguiente se muestra el atributo **ua**:

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

El valor de la opción **ua** se debe especificar entre comillas.

Control de acceso

Si se activa el parámetro <Phone-UI-User-Mode>, la interfaz gráfica de usuario de teléfono admite el atributo de acceso de usuario de los parámetros relevantes si la interfaz gráfica de usuario presenta un elemento de menú.

Para las entradas de menú que están asociadas con un parámetro de configuración único:

- Si se proporciona el parámetro con "ua = na" atributo ("ua" significa "acceso de usuario") la entrada desaparece.
- Si se proporciona el parámetro con el atributo "ua = ro" se hace que la entrada sea de solo lectura y no editable.

Para las entradas de menú que están asociadas con varios parámetros de configuración:

- Si se proporcionan todos los parámetros en cuestión con el atributo "ua = na" las entradas desaparecen.

Temas relacionados

Control de acceso de configuración, en la página 9

Propiedades de parámetros

Estas propiedades se aplican a los parámetros:

- Los parámetros que no se especifican mediante un perfil se dejan sin modificar en el teléfono.
- Se ignorarán los parámetros no reconocidos.
- Si el perfil de formato abierto contiene varias repeticiones de la misma etiqueta de parámetro, la última repetición tiene prioridad sobre las anteriores. Para evitar el reemplazo involuntario de valores de configuración de un parámetro, se recomienda que cada perfil especifique como máximo una instancia de un parámetro.
- El último perfil procesado tendrá preferencia. Si varios perfiles especifican el mismo parámetro de configuración, el valor del último perfil tiene prioridad.

Formatos de cadena

Estas propiedades se aplican al formato de las cadenas:

- Se permiten los comentarios mediante la sintaxis XML estándar.

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

- Los espacios en blanco iniciales y finales se permiten para facilitar la lectura, pero se quitarán del valor del parámetro.
- Las nuevas líneas dentro de un valor se convierten en espacios.
- Se permite un encabezado XML con el formato `<? ?>`, pero el teléfono lo ignora.
- Para introducir caracteres especiales, utilice caracteres de escape de XML básicos, tal y como se muestra en la tabla siguiente.

Carácter especial	Secuencia de escape XML
& (ampersand)	&
< (menor que)	<
> (mayor que)	>
' (apóstrofo)	'
" (comillas dobles)	"

En el ejemplo siguiente, se introducen secuencias de carácter de escape para representar los símbolos mayor que y menor que, necesarios en una regla de plan de marcación. En este ejemplo se define un plan de marcación de línea directa de información que establece el parámetro <Dial_Plan_1_> (**Inicio de sesión de Admin** > **Avanzado** > **Voz** > **Ext (n)**) igual a (S0 <:18005551212>).

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

- Los caracteres numéricos de escape, que utilizan valores decimales y hexadecimales (s.a. `(` y `.`), se traducen.
- El firmware del teléfono solo admite caracteres ASCII.

Compresión y cifrado de perfil abierto (XML)

Puede comprimir el perfil de configuración abierta para reducir la carga de red en el servidor de aprovisionamiento. También puede cifrarse el perfil para proteger la información confidencial. La compresión no es necesaria, pero debe preceder al cifrado.

Temas relacionados

Formatos de perfil de configuración, en la página 15

Compresión de perfil abierto

El método de compresión compatible es el algoritmo de deflación gzip (RFC1951). La utilidad gzip y la biblioteca de compresión que implementa el mismo algoritmo (zlib) están disponibles en sitios de Internet.

Para identificar la compresión, el teléfono espera que el archivo comprimido contenga un encabezado compatible con gzip. La invocación de la utilidad gzip en el perfil abierto original genera el encabezado. El teléfono examina el encabezado del archivo descargado para determinar el formato de archivo.

Por ejemplo, si `profile.xml` es un perfil válido, el archivo `profile.xml.gz` también se acepta. Cualquiera de los siguientes comandos puede generar este tipo de perfil:

- `>gzip profile.xml`

  Sustituirá el archivo original con el archivo comprimido.

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

  Deja el archivo original en su lugar, crea el nuevo archivo comprimido.

Se proporciona un tutorial sobre la compresión en la sección Compresión de un perfil abierto con Gzip, en la página 67.

Temas relacionados

Compresión de un perfil abierto con Gzip, en la página 67

Cifrado de perfil abierto

Puede utilizarse el cifrado de claves simétricas para cifrar un perfil de configuración abierto, independientemente de si el archivo está comprimido. Compresión, si se aplica, se debe aplicar antes del cifrado.

El servidor de aprovisionamiento utiliza HTTPS para gestionar el aprovisionamiento inicial del teléfono tras la implementación. El cifrado previo de los perfiles de configuración fuera de línea permite el uso de HTTP para resincronizar perfiles. Esto reduce la carga en el servidor HTTPS en las implementaciones a gran escala.

El teléfono admite dos métodos de cifrado de archivos de configuración:

- Cifrado AES-256-CBC
- Cifrado de contenido HTTP basado en RFC 8188 con cifrado AES-128-GCM

La clave o Input Keying Material (IKM) se debe aprovisionar previamente en la unidad. La secuencia de inicio de la clave puede lograrse de forma segura mediante HTTPS.

El nombre de archivo final no necesita un formato específico, pero un nombre de archivo que termina con la extensión `.cfg` suele indicar un perfil de configuración.

Cifrado AES-256-CBC

El teléfono admite el cifrado AES-256-CBC de archivos de configuración.

La herramienta de cifrado OpenSSL disponible para su descarga en varios sitios de Internet, puede realizar el cifrado. La compatibilidad con cifrado AES de 256 bits puede requerir la recopilación de la herramienta para habilitar el código AES. El firmware se ha probado con la versión openssl-0.9.7c.

Cifrado de un perfil con OpenSSL, en la página 68 proporciona un tutorial sobre el cifrado.

Para un archivo cifrado, el perfil espera que el archivo tenga el mismo formato que el generado por el comando siguiente:

```
# 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
```

-k en minúsculas precede la clave secreta, que puede ser cualquier frase de texto sin formato y que se utiliza para generar una sal aleatoria de 64 bits. Con el secreto especificado por el argumento -k, la herramienta de cifrado obtiene un vector inicial de 128 bits aleatorio y la clave de cifrado de 256 bits real.

Cuando se usa este método de cifrado de un perfil de configuración, se debe informar al teléfono del valor de la clave secreta para descifrar el archivo. Este valor se especifica como calificador en la URL de perfil. La sintaxis es la siguiente, mediante una dirección URL explícita:

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

Este valor se programa con uno de los parámetros de Profile_Rule.

Temas relacionados

Cifrado de un perfil con OpenSSL, en la página 68

Expansión de macro

Varios parámetros de abastecimiento experimentan una expansión de marco internamente antes de que se evalúe. Este paso de evaluación previa ofrece una mayor flexibilidad en el control de las actividades de resincronización y actualización del teléfono.

Estos grupos de parámetros experimentan una expansión de macro antes de la evaluación:

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

En determinadas circunstancias, algunos parámetros de uso generales (GPP_*) también experimentan una expansión de macro, tal como se indica explícitamente en la sección Argumentos de resincronización opcional, en la página 25.

Durante la expansión de macro, el contenido de las variables con nombre reemplaza expresiones del formulario $NAME y $(NAME). Estas variables incluyen parámetros generales, varios identificadores de producto, determinados temporizadores de evento y los valores de estado de aprovisionamiento. Para obtener una lista completa, consulte Variables de expansión de macro, en la página 78.

En el siguiente ejemplo, la expresión $(MAU) se utiliza para insertar la dirección MAC 000E08012345.

El administrador escribe: **`$(MAU)config.cfg`**

La expansión de macro resultante para un dispositivo con la dirección MAC de dispositivo 000E08012345 es: `000E08012345config.cfg`

Si no se reconoce el nombre de la macro, permanece sin expandir. Por ejemplo, no se reconoce el nombre STRANGE como nombre de macro válido, mientras que MAU sí se reconoce como nombre de macro válido.

El administrador escribe: **`$STRANGE$MAU.cfg`**

La expansión de macro resultante para un dispositivo con la dirección MAC de dispositivo 000E08012345 es: `$STRANGE000E08012345.cfg`

La expansión de macro no se aplicará recursivamente. Por ejemplo, $$MAU" se expande $MAU" ($$ se expande) y no tiene como resultado la dirección MAC.

El contenido de los parámetros de propósito especial, GPP_SA a GPP_SD, se asignan a las expresiones de macro de $SA a $SD. Estos parámetros solo son una expansión de macro como argumento de las opciones **--key**, **--uid** y **--pwd** en una URL de resincronización.

Expresiones condicionales

Las expresiones condicionales pueden activar eventos de resincronización y seleccionar de URL alternativas para las operaciones de resincronización y actualización.

Las expresiones condicionales están formadas por una lista de comparaciones, separadas por el operador **and**. Todas las comparaciones deben cumplirse para que la condición sea verdadera.

Cada comparación puede relacionarse con uno de los siguientes tres tipos de literales:

- Valores enteros
- Números de versión de software o hardware
- Cadenas entre comillas dobles

Números de versión

La versión de software publicada formalmente de los teléfonos multiplataforma (MPP) utilizan este formato, donde BN=Número de versión:

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

La cadena de comparación debe usar el mismo formato. De lo contrario, se produce un error de análisis de formato.

En la versión de software, v1-v2-v3-v4 pueden especificar diferentes dígitos y caracteres, pero debe empezar con un dígito. Al comparar la versión de software, v1-v2-v3-v4 se comparan en secuencia y los dígitos de más a la izquierda prevalen sobre los posteriores.

Si v[x] incluye solo dígitos, se comparan los dígitos; si v[x] incluye dígitos + caracteres alfabéticos, los dígitos se comparan en primer lugar y, a continuación, se comparan caracteres en orden alfabético.

Ejemplo de número de versión válido

sipyyyy.11-0-0MPP-BN

Por el contrario: 11.0.0 es un formato no válido.

Comparación

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

Las cadenas entre comillas se pueden comparar en busca de igualdad o desigualdad. Los enteros y los números de versión también se pueden comparar aritméticamente. Los operadores de comparación pueden expresarse como símbolos o como acrónimos. Los acrónimos son útiles para expresar la condición en un perfil de formato abierto.

Operador	Sintaxis alternativa	Descripción	Aplicable a enteros y operandos de versión	Aplicable a los operandos de cadena entre comillas
=	eq	igual que	Sí	Sí
!=	ne	no igual a	Sí	Sí
<	lt	menor que	Sí	No
<=	le	menor o igual que	Sí	No
>	gt	mayor que	Sí	No
>=	ge	mayor o igual que	Sí	No
Y		y	Sí	Sí

Es importante incluir las variables de macro entre comillas dobles cuando se espera un literal de cadena. No lo haga cuando se espere un número o un número de versión.

Cuando se utiliza en el contexto de los parámetros Profile_Rule* y Upgrade_Rule, las expresiones condicionales deben incluirse en la sintaxis "(expr)?" como en este ejemplo de regla de actualización. Recuerde que BN indica el número de compilación.

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

No utilice la sintaxis anterior con paréntesis para configurar los parámetros de Resync_Trigger_*.

Sintaxis de la dirección URL

Utilice la sintaxis de dirección URL estándar para especificar cómo se pueden recuperar los archivos de configuración y las cargas de firmware en los parámetros Profile_Rule* y Upgrade_Rule, respectivamente. La sintaxis es la siguiente:

[esquema://] [servidor [:puerto]] ruta del archivo

Donde **esquema** es uno de estos valores:

- tftp
- http
- https

Si **esquema** se omite, se utiliza tftp. El servidor puede ser un nombre de host reconocido por DNS o una dirección IP numérica. El puerto es el número de puerto de destino UDP o TCP. La ruta del archivo debe comenzar con el directorio raíz (/); debe ser una ruta de acceso absoluta.

Si falta **servidor**, el servidor tftp se especifica a través de DHCP (opción 66).

Nota Para las reglas de actualización, debe especificarse el servidor.

Si falta **puerto**, se utiliza el puerto estándar para el esquema especificado. Tftp usa el puerto UDP 69, http utiliza el puerto TCP 80, https utiliza el puerto TCP 443.

Debe estar presente una ruta del archivo. No necesita referirse necesariamente a un archivo estático, pero puede indicar el contenido dinámico que se ha obtenido a través de CGI.

La expansión de macro se aplica dentro de las direcciones URL. A continuación se muestran ejemplos de direcciones URL válidas:

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

Cuando se utiliza la opción 66 de DHCP, las reglas de actualización no admiten una sintaxis vacía. Solo es aplicable para la regla de perfil*.

Cifrado de contenido de HTTP basado en RFC 8188

El teléfono admite el cifrado de contenido HTTP basado en RFC 8188 con cifrado AES-128-GCM para los archivos de configuración. Con este método de cifrado, cualquier entidad puede leer los encabezados de mensaje HTTP. Sin embargo, solo las entidades que conocen Input Keying Material (IKM) pueden leer la carga. Si el teléfono se suministra con IKM, el teléfono y el servidor de aprovisionamiento pueden intercambiar archivos de configuración de forma segura, a la vez que permiten que elementos de la red de terceros utilicen los encabezados de mensaje para fines de supervisión y análisis.

El parámetro de configuración XML **`IKM_HTTP_Encrypt_Content`** contiene el IKM en el teléfono. Por motivos de seguridad, este parámetro no es accesible en la página web de administración de teléfono. Tampoco es visible en el archivo de configuración del teléfono, al que se puede tener acceso desde la dirección IP del teléfono o desde los informes de configuración del teléfono enviados al servidor de aprovisionamiento.

Si desea utilizar el cifrado basado en RFC 8188, asegúrese de lo siguiente:

- Aprovisionar el teléfono con el IKM especificando el IKM con el parámetro XML **`IKM_HTTP_Encrypt_Content`** en el archivo de configuración que se envía desde el servidor de aprovisionamiento al teléfono.
- Si este cifrado se aplica a los archivos de configuración que se envían desde el servidor de aprovisionamiento al teléfono, asegúrese de que el encabezado HTTP de *codificación de contenido* del archivo de configuración tiene «aes128gcm».

  En la ausencia de este encabezado, el método AES-256-CBC tiene prioridad. El teléfono aplica descifrado AES-256-CBC si una clave AES-256-CBC se encuentra en una regla de perfil, independientemente de IKM.
- Si desea que el teléfono aplique el cifrado a los informes de la configuración que envía al servidor de aprovisionamiento, asegúrese de que no hay ninguna clave AES-256-CBC especificada en la regla de informe.

Argumentos de resincronización opcional

Los argumentos opcionales, **`key`**, **`uid`** y **`pwd`** pueden preceder a las direcciones URL introducidas en los parámetros Profile_Rule*, de manera colectiva entre corchetes.

key

La opción **`--clave`** indica al teléfono que el archivo de configuración que recibe desde el servidor de aprovisionamiento se cifra mediante cifrado AES-256-CBC, a no ser que en encabezado de *codificación de contenido* del archivo indique cifrado «aes128gcm». La propia clave se especifica como una cadena tras el término **`--clave`**. También se puede incluir la clave de cifrado entre comillas (") opcionalmente. El teléfono usa la clave para descifrar el archivo de configuración.

Ejemplos de uso

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

Los argumentos opcionales entre corchetes son una macro expandida. Los parámetros del propósito especial, GPP_SA a GPP_SD, se expanden mediante macros en las variables de macro, $SA a $SD, solo cuando se utilizan como argumentos de la opción de clave. Consulte estos ejemplos:

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

En los perfiles de formato abierto, el argumento de **--key** debe ser el mismo que el argumento para la opción **-k** que se asigna a **openssl** .

uid y pwd

Las opciones **uid** y **pwd** pueden utilizarse para especificar el ID de usuario y la autenticación de contraseña para la dirección URL especificada. Los argumentos opcionales entre corchetes son una macro expandida. Los parámetros del propósito especial, GPP_SA a GPP_SD, se expanden mediante macros en las variables de macro, $SA a $SD, solo cuando se utilizan como argumentos de la opción de clave. Consulte estos ejemplos:

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

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

a continuación, se expande a:

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

Aplicar un perfil al dispositivo de telefonía IP

Después de crear una secuencia de comandos de configuración XML, se debe pasar al teléfono para la aplicación. Para aplicar la configuración, puede descargar el archivo de configuración al teléfono desde un servidor TFTP, HTTP o HTTPS mediante un explorador web o mediante la utilidad cURL de la línea de comandos.

Descarga del archivo de configuración en el teléfono desde un servidor TFTP

Realice estos pasos para descargar el archivo de configuración en una aplicación de servidor TFTP de su PC.

Procedimiento

Paso 1 Conecte el PC a la LAN del teléfono.

Paso 2 Ejecute una aplicación de servidor TFTP en el PC y asegúrese de que el archivo de configuración esté disponible en el directorio raíz TFTP.

Paso 3 En un explorador web, introduzca la dirección IP de la LAN del teléfono, la dirección IP del equipo, el nombre de archivo y las credenciales de inicio de sesión. Utilice este formato:

http://<Dirección_IP_WAN>/admin/resync?tftp://<Dirección_IP_PC>/<nombre_archivo>&user=admin&password=<contraseña>

Ejemplo:

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

Descarga del archivo de configuración del teléfono con cURL

Realice estos pasos para descargar la configuración para el teléfono mediante cURL. Esta herramienta de la línea de comandos se usa para transferir datos con una sintaxis de la dirección URL. Para descargar cURL, visite:

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

Nota Se recomienda no utilizar cURL para publicar la configuración en el teléfono porque el nombre de usuario y la contraseña se pueden capturar mientras usa cURL.

Procedimiento

Paso 1 Conecte el PC al puerto LAN del teléfono.

Paso 2 Descargue el archivo de configuración para el teléfono introduciendo el siguiente comando de cURL:

```
curl -d @my_config.xml
"http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin"
```

Parámetros de aprovisionamiento

En esta sección se describen los parámetros de aprovisionamiento organizados de forma general según la función:

Existen estos tipos de parámetros de aprovisionamiento:

- De uso general
- Activaciones
- Factores que favorecen VDI
- Programaciones configurables
- Reglas de perfil
- Regla de actualización

Parámetros de uso general

Los parámetros GPP_* de uso general (**Inicio de sesión de Admin** > **Avanzado** > **Voz** > **Aprovisionamiento**) se utilizan como registros de cadena gratis cuando se configura el teléfono para interactuar con una solución

de servidor de aprovisionamiento particular. Los parámetros GPP_* están vacíos de forma predeterminada. Se pueden configurar para que incluyan varios valores, como estos:

- Claves de cifrado
- URL
- Información de estado de aprovisionamiento multifase
- Plantillas de solicitudes posteriores
- Asignaciones de alias de nombre de parámetro
- Valores de cadena parcial, combinados al final en valores de parámetros completos

Los parámetros GPP_* están disponibles para la expansión de macros en otros parámetros de aprovisionamiento. Con esta finalidad, los nombres de macro en mayúsculas de una sola letra (A a P) son suficientes para identificar el contenido de GPP_A a GPP_P. Asimismo, los nombres de macro en mayúsculas de dos letras SA a SD identifican de GPP_SA a GPP_SD como un caso especial cuando se usan como argumentos de las siguientes opciones de direcciones URL:

key, **uid** y **pwd**

Estos parámetros pueden utilizarse como variables en reglas de actualización y aprovisionamiento. Se hace referencia a ellos estableciendo como prefijo en el nombre de la variable el carácter '$', como $GPP_A.

Utilización de parámetros de uso general

Por ejemplo, si GPP_A contiene la cadena ABC y GPP_B contiene 123, la macro de expresión A B se expande en ABC123.

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Seleccione **Voz** > **Aprovisionamiento**.

Paso 2 Desplácese hasta la sección **Parámetros de uso general**.

Paso 3 Introduzca los valores válidos en los campos, de GPP A a GPP P.

Paso 4 Haga clic en **Enviar todos los cambios**.

Activaciones

Los parámetros Provision_Enable y Upgrade_Enable controlan todas las operaciones de resincronización del perfil y actualización de firmware. Estos parámetros controlan resincronizaciones y actualizaciones de manera independiente entre sí. Estos parámetros también controlan los comandos de resincronización y actualización que se emiten a través del servidor web de administración. Estos parámetros se establecen en **Sí** de forma predeterminada.

El parámetro Resync_From_SIP controla las solicitudes de operaciones de resincronización. Se envía un evento SIP NOTIFY desde el servidor proxy del proveedor del servicio al teléfono. Si está activado, el proxy puede solicitar una resincronización. Para ello, el proxy envía un mensaje SIP NOTIFY que contiene el evento: encabezado de resincronización al dispositivo.

El dispositivo comprueba la solicitud con una respuesta 401 (autorización rechazada para las credenciales usadas). El dispositivo espera una solicitud posterior autenticada antes de aceptar la solicitud de resincronización del proxy. Los encabezados Event: reboot_now y Event: restart_now realizan reinicios en fío y en caliente, respectivamente, que también se comprueban.

Las dos activaciones restantes son Resync_On_Reset y Resync_After_Upgrade_Attempt. Estos parámetros determinan si el dispositivo realiza una operación de resincronización después de reinicios de software de encendido y después de cada intento de actualización.

Cuando se activa Resync_On_Reset, el dispositivo presenta un retraso aleatorio que sigue la secuencia de arranque antes de realizar el restablecimiento. El retraso es un tiempo aleatorio hasta el valor que especifica la Resync_Random_Delay (en segundos). En un grupo de teléfonos que se encienden al mismo tiempo, este retraso se propaga a la hora de inicio de las solicitudes de resincronización de cada unidad. Esta función puede resultar útil en una gran implementación residencial, en caso de que se produzcan cortes de energía regionales.

Factores que favorecen VDI

El teléfono permite resincronizar a intervalos específicos o a una hora concreta.

Resincronización a intervalos específicos

El teléfono se ha diseñado para resincronizar con el servidor de aprovisionamiento de forma periódica. El intervalo de resincronización se configura en Resync_Periodic (segundos). Si el valor se deja vacío, el dispositivo no se resincroniza periódicamente.

La resincronización suele realizarse cuando las líneas de voz están inactivas. Si una línea de voz está activa y hay prevista una resincronización, el teléfono retrasa el proceso de resincronización hasta que la línea vuelve a estar inactiva. Una resincronización puede provocar que los valores del parámetro de configuración cambien.

Una operación de resincronización puede fallar porque el teléfono no puede recuperar un perfil desde el servidor, el archivo descargado está dañado o se ha producido un error interno. El dispositivo intenta volver a resincronizarse tras el tiempo especificado en Resync_Error_Retry_Delay (segundos). Si Resync_Error_Retry_Delay se ajusta en 0, el dispositivo no intenta resincronizar de nuevo tras un intento fallido de resincronización.

Si se produce un error en una actualización, se realiza un reintento tras los segundos de Upgrade_Error_Retry_Delay.

Hay disponibles dos parámetros configurables para desencadenar condicionalmente una sincronización: Resync_Trigger_1 y Resync_Trigger_2. Cada parámetro se puede programar con una expresión condicional que experimenta una expansión de macro. Cuando caduca el intervalo de resincronización (tiempo para la resincronización siguiente) los desencadenadores, si se han establecido, evitarán la resincronización a no ser que uno o más desencadenadores se evalúen como verdaderos.

La siguiente condición de ejemplo desencadena una resincronización. En el ejemplo, han transcurrido más de 5 minutos (300 segundos) desde el último intento de actualización del teléfono y han transcurrido al menos 10 minutos (600 segundos) desde el último intento de resincronización.

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

Resincronización a una hora concreta

El parámetro Resync_At permite al teléfono resincronizar a una hora concreta. Este parámetro usa el formato de 24 horas (hhmm) para especificar la hora.

El parámetro Resync_At_Random_Delay permite al teléfono resincronizar con un retraso de tiempo sin especificar. Este parámetro utiliza un formato de número entero positivo para especificar la hora.

Debe evitar inundar el servidor con solicitudes de resincronización de varios teléfonos que se han definido para resincronizar al mismo tiempo. Para ello, el teléfono activa la resincronización hasta 10 minutos después de la hora especificada.

Por ejemplo, si establece la hora de resincronización 1000 (10 a.m.), el teléfono activa la resincronización en cualquier momento entre las 10:00 y las 10:10 a.m.

Esta función está desactivada de forma predeterminada. Si se aprovisiona el parámetro Resync_At, se ignora el parámetro Resync_Periodic.

Programaciones configurables

Puede configurar programaciones para resincronizaciones periódicas y puede especificar los intervalos de reintento de resincronización y los fallos de actualización mediante estos parámetros de abastecimiento:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Cada parámetro acepta un único valor de retraso (en segundos). La nueva sintaxis extendida permite obtener una lista separada por comas de elementos de retraso consecutivos. El último elemento de la secuencia se repite de forma implícita de forma permanente.

De manera opcional, puede usar un signo más para especificar otro valor numérico que agrega un retraso aleatorio adicional.

Ejemplo 1

En este ejemplo, el teléfono resincroniza periódicamente cada 2 horas. Si se produce un error de resincronización, el dispositivo vuelve a intentarlo a estos intervalos: 30 minutos, 1 hora, 2 horas, 4 horas. El dispositivo sigue intentándolo en intervalos de 4 horas hasta que resincroniza correctamente.

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

Ejemplo 2

En este ejemplo, el dispositivo resincroniza periódicamente cada hora (más un retraso aleatorio adicional de hasta 10 minutos). En caso de error de resincronización, el dispositivo vuelve a intentarlo a estos intervalos: 30 minutos (además de hasta 5 minutos). 1 hora (además de hasta 10 minutos), 2 horas (además de hasta 15 minutos). El dispositivo sigue intentándolo en intervalos de 2 horas (además de hasta 15 minutos) hasta que resincroniza correctamente.

```
Resync_Periodic=3600+600
```

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

Ejemplo 3

En este ejemplo, si se produce un error en un intento de actualización remoto, el dispositivo vuelve a intentar la actualización en 30 minutos y, a continuación, de nuevo tras una hora más y después tras dos horas. Si la actualización sigue resultando errónea, el dispositivo lo reintenta cada cuatro o cinco horas hasta que la actualización tiene éxito.

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

Reglas de perfil

El teléfono proporciona varios parámetros de perfil de configuración remota (Profile_Rule*). Por lo tanto, cada operación de resincronización puede recuperar varios archivos administrados por varios servidores.

En el escenario más sencillo, el dispositivo se resincroniza periódicamente con un solo perfil en un servidor central, que actualiza todos los parámetros internos pertinentes. Como alternativa, el perfil se puede dividir entre diferentes archivos. Un archivo es común para todos los teléfonos de una implementación. Se proporciona un único archivo independiente para cada cuenta. Las claves de cifrado y la información de certificado se pueden proporcionar mediante otro perfil, almacenado en un servidor independiente.

Cada vez que vence una operación de resincronización, el teléfono evalúa los cuatro parámetros Profile_Rule* en secuencia:

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

Cada evaluación puede tener como resultado la recuperación de un perfil de un servidor de aprovisionamiento remoto, con una posible actualización de algunos parámetros internos. Si se produce un error en una evaluación, la secuencia de resincronización se interrumpe y se vuelve a intentar desde el principio especificado por el parámetro Resync_Error_Retry_Delay (segundos). Si todas las evaluaciones se realizan correctamente, el dispositivo espera a la segunda resincronización especificada por el parámetro Resync_Periodic y, a continuación, realiza otra resincronización.

El contenido de cada parámetro Profile_Rule* está compuesto por un conjunto de alternativas. Las alternativas se separan mediante el carácter | (barra vertical). Cada alternativa consiste en una expresión condicional, una expresión de asignación, una URL de perfil y todas las opciones URL asociadas. Todos estos componentes son opcionales dentro de cada alternativa. Estas son las combinaciones válidas y el orden en que deben aparecer si están presentes:

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

Dentro de los parámetros de Profile_Rule*, todas las alternativas excepto la última deben proporcionar una expresión condicional. Esta expresión se evalúa y se procesa como sigue:

1. Las condiciones se evalúan de izquierda a derecha, hasta que se encuentra una que se evalúa como verdadera (o hasta que se encuentra una alternativa sin expresión condicional).

2. Se evalúa cualquier expresión de asignación adjunta, si está presente.
3. Si se especifica una dirección URL como parte de esa alternativa, se intenta descargar el perfil que se encuentra en la dirección URL especificada. El sistema intenta actualizar los parámetros internos en consecuencia.

Si todas las alternativas tienen expresiones condicionales y ninguna se evalúa como verdadera (o si la regla del perfil completo está vacía), se omite el parámetro Profile_Rule*. Se evalúa el siguiente parámetro de regla de perfil en la secuencia.

Ejemplo 1

En este ejemplo se resincroniza incondicionalmente con el perfil en la dirección URL especificada y se realiza una solicitud GET de HTTP al servidor de aprovisionamiento remoto:

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

Ejemplo 2

En este ejemplo, el dispositivo se resincroniza con dos direcciones URL diferentes, según el estado de registro de la línea 1. En caso del registro perdido, el dispositivo ejecuta POST HTTP a una secuencia de comandos CGI. El dispositivo envía el contenido de la macro expandida GPP_A, que puede proporcionar información adicional sobre el estado del dispositivo:

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

Ejemplo 3

En este ejemplo, el dispositivo se resincroniza con el mismo servidor. El dispositivo proporciona información adicional, si un certificado no está instalado en la unidad (en las unidades de previas a 2.0 heredadas):

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

Ejemplo 4

En este ejemplo, la línea 1 está desactivada hasta que GPP_A se aprovisiona a través de la primera URL. Después, se resincroniza a la segunda dirección URL:

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

Ejemplo 5

En este ejemplo, se supone que el perfil que el servidor devuelve contiene etiquetas de elementos XML. Estas etiquetas deben reasignarse a los nombres de parámetro adecuados mediante la asignación de alias que se almacena en GPP_B:

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

Normalmente se considera que una resincronización no se ha realizado correctamente si no se recibe un perfil solicitado del servidor. El parámetro Resync_Fails_On_FNF puede omitir este comportamiento predeterminado. Si Resync_Fails_On_FNF se ajusta en No, el dispositivo acepta una respuesta file-not-found (archivo no encontrado) del servidor como resincronización correcta. El valor predeterminado de Resync_Fails_On_FNF es Yes (Sí).

Regla de actualización

La Regla de actualización indica al dispositivo que se active para una nueva carga y de dónde la carga, si fuera necesario. Si la carga ya está en el dispositivo, no intenta obtenerla. Por lo tanto, la validez de la ubicación de carga no importa si la carga deseada se encuentra en la partición inactiva.

Upgrade_Rule especifica un firmware que, si es diferente de la carga actual, se descargará y se aplicará a no ser que esté limitado por una expresión condicional o que Upgrade_Enable se establezca en **No**.

El teléfono proporciona un parámetro de actualización remoto configurable, Upgrade_Rule. Este parámetro acepta la sintaxis similar a los parámetros de regla de perfil. No se admiten opciones de URL para las actualizaciones, pero se pueden usar expresiones condicionales y expresiones de asignación. Si se utilizan expresiones condicionales, el parámetro se puede rellenar con varias alternativas, separadas por el carácter |. La sintaxis para cada alternativa es la siguiente:

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

Al igual que en el caso de los parámetros de Profile_Rule*, el parámetro Upgrade_Rule evalúa cada alternativa hasta que se cumpla una expresión condicional o una alternativa no tenga ninguna expresión condicional. Se evalúa cualquier expresión de asignación adjunta, si se especifica. A continuación, se intenta realizar una actualización a la dirección URL especificada.

Si Upgrade_Rule contiene una dirección URL sin una expresión condicional, el dispositivo se actualiza a la imagen del firmware que especifica la dirección URL. Después de la expansión de macro y de la evaluación de la regla, el dispositivo no vuelve a intentar la actualización hasta que se modifique la regla o se cambie la combinación efectiva de esquema + servidor + puerto + ruta del archivo.

Para intentar una actualización del firmware, el dispositivo desactiva el audio al inicio del procedimiento y se reiniciará al final del procedimiento. El dispositivo iniciará automáticamente una actualización que se basa en el contenido de Upgrade_Rule solo si todas las líneas de voz están inactivas actualmente.

Por ejemplo,

- Para el Cisco IP serie 6800:

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

  where BN==Build Number
  ```

En este ejemplo, Upgrade_Rule actualizará el firmware a la imagen que se almacena en la dirección URL indicada.

Aquí se ofrece otro ejemplo de los teléfonos Cisco IP Phone serie 6800:

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

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

where BN==Build Number
```

En este ejemplo se dirige la unidad para cargar una de las dos imágenes, basándose en el contenido de un parámetro de uso general, GPP_F.

El dispositivo puede aplicar un límite para volver a una versión anterior del número de revisión del firmware, que puede ser una opción de personalización útil. Si está configurado un número de revisión del firmware válida en el parámetro Downgrade_Rev_Limit, el dispositivo rechaza los intentos de actualización para versiones de firmware anteriores al límite especificado.

Tipos de datos

Estos tipos de datos se utilizan con los parámetros de configuración de perfil:

- {a, b, c...}: una opción entre a, b, c...
- Bool: valor booleano "sí" o "no".
- CadScript: una secuencia de comandos mini que especifica los parámetros de la cadencia de una señal. Hasta 127 caracteres.

  Sintaxis: $S_1[;S_2]$, donde:

  - $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ y se conoce como una sección.
  - $on_{i,j}$ y $off_{i,j}$ son la duración de on/off en segundos de un *segmento*. i = 1 o 2 y j = 1 a 6.
  - D es la duración total de la sección en segundos.

  Todas las duraciones pueden tener un máximo de tres decimales para proporcionar una resolución de 1 ms. El carácter comodín "*" significa duración infinita. Los segmentos de una sección se reproducen en orden y se repiten hasta que se reproduce la duración total.

  Ejemplo 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
  ```

  Ejemplo 2: timbre distintivo (corto, corto, corto, largo):

  ```
  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: sintaxis de secuencia de comandos que se usa para especificar los planes de marcación Line 1 (Línea 1) y Line 2 (Línea 2).
- Float<n>: valor de coma flotante con un máximo de n decimales.
- FQDN: nombre de dominio completo. Puede contener hasta 63 caracteres. A continuación se muestran ejemplos:
  - sip.Cisco.com:5060 o 109.12.14.12:12345
  - sip.Cisco.com o 109.12.14.12
- FreqScript: un miniscript que especifica los parámetros de frecuencia y de nivel de un tono. Contiene un máximo de 127 caracteres.

  Sintaxis: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, donde:
  - F_1–F_6 son la frecuencia en Hz (solo enteros sin signo).
  - L_1– L_6 son los niveles correspondientes en dBm (con un máximo de un decimal).

  Se permiten espacios en blanco antes y después de la coma, pero no se recomienda.

  Ejemplo 1: Tono de espera de llamada:

```
440@-10

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

  Ejemplo 2: tono de marcación:

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

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

- IP: dirección IPv4 válida en forma de x.x.x.x, donde la x está entre 0 y 255. Ejemplo: 10.1.2.100.
- ID de usuario: ID de usuario, tal y como aparece en una dirección URL; hasta 63 caracteres.
- Teléfono: una cadena de número de teléfono, como 14081234567, *69, *72, 345678; o una URL genérica, por ejemplo, 1234@10.10.10.100:5068 o jsmith@Cisco.com. La cadena puede contener hasta 39 caracteres.
- PhTmplt: una plantilla de números de teléfono. Cada plantilla puede contener uno o varios de los patrones que están separados por una coma (,). Los espacios en blanco al principio de cada trama se ignoran. "?" y "*" representan los caracteres comodín. Para representar literalmente, utilice %xx. Por ejemplo, %2a representa *. La plantilla puede contener hasta 39 caracteres. Ejemplos: “1408*, 1510*”, “1408123????, 555?1.”.
- Puerto: el número de puerto TCP/UDP (0-65535). Se puede especificar en formato decimal o hexadecimal.

- ProvisioningRuleSyntax: sintaxis de secuencias de comandos que se utiliza para definir la resincronización de configuración y las reglas de actualización de firmware.
- PwrLevel: el nivel de potencia se expresa en dBm con un decimal, por ejemplo, –13,5 o 1,5 (dBm).
- RscTmplt: una plantilla de código de estado de respuesta SIP, por ejemplo, "404, 5*", "61?", “407, 408, 487, 481”. Puede contener hasta 39 caracteres.
- Sig<n>: valor con signo de n bits. Se puede especificar en formato decimal o hexadecimal. El signo "-" debe preceder a los valores negativos. El signo + antes de los valores positivos es opcional.
- Códigos de asterisco: código de activación de un servicio adicional, como *69. El código puede contener hasta 7 caracteres.
- Str<n>: una cadena genérica con un máximo de n caracteres no reservados.
- Tiempo<n>: tiempo de duración en segundos, con un máximo de n decimales. Se ignorarán los decimales adicionales especificados.
- ToneScript: un miniscript que especifica los parámetros de frecuencia, nivel y cadencia de un tono de llamada en curso. La secuencia de comandos puede contener hasta 127 caracteres.

  Sintaxis: FreqScript;Z_1[;Z_2].

  La sección Z_1 es similar a S_1 de un CadScript, con la excepción que cada segmento on/off va seguido de un parámetro de componentes de frecuencia: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ donde:

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ especifica los componentes de frecuencia en la FreqScript que se utilizan en ese segmento.

  Si se utiliza más de un componente de frecuencia en un segmento, los componentes se suman juntos.

  Ejemplo 1: tono de marcación:

```
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
```

  Ejemplo 2: Tono entrecortado:

```
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 de n bits sin signo, donde n = 8, 16 o 32. Se puede especificar en formato decimal o hexadecimal, por ejemplo, 12 o 0x18, siempre y cuando el valor encaje en n bits.

Nota Tenga esto en cuenta:

- <Par Name> representa un nombre de parámetro de configuración. En un perfil, la etiqueta correspondiente se forma al reemplazar el espacio con un guion bajo "_", por ejemplo, **Par_Name**.
- Un campo de valor predeterminado vacío implica una cadena vacía < “” >.
- El teléfono sigue usando los últimos valores configurados para las etiquetas que no están presentes en un perfil específico.
- Las plantillas se comparan en el orden indicado. Se selecciona la primera concordancia *no la más cercana*. El nombre del parámetro debe coincidir exactamente.
- Si se proporciona más de una definición de un parámetro en un perfil, la última de tales definiciones en el archivo es la que tendrá efecto en el teléfono.
- La especificación de un parámetro con un valor de parámetro vacío fuerza el parámetro a su valor predeterminado. Para especificar una cadena vacía en su lugar, utilice la cadena vacía "" como el valor del parámetro.

Actualizaciones de perfil y actualizaciones de firmware

El teléfono admite el aprovisionamiento remoto seguro (configuración) y las actualizaciones de firmware. Un teléfono no aprovisionado puede recibir un perfil cifrado diseñado para ese dispositivo. El teléfono no requiere una clave explícita debido a un mecanismo seguro de aprovisionamiento por primera vez que utiliza la funcionalidad SSL.

No es necesaria la intervención del usuario para iniciar o finalizar una actualización de perfil o de firmware, o si las actualizaciones intermedias son necesarias para alcanzar una futura actualización de estado desde una versión anterior. Una resincronización de perfil se intenta solo cuando el teléfono está inactivo, ya que una resincronización puede desencadenar un reinicio del software y puede desconectar una llamada.

Los parámetros generales administran el proceso de aprovisionamiento. Todos los teléfonos pueden configurarse para ponerse en contacto periódicamente con un servidor de aprovisionamiento normal (NPS). La comunicación con NPS no necesita el uso de un protocolo seguro porque el perfil actualizado se cifra mediante una clave de secreto compartido. El NPS puede ser un servidor TFTP, HTTP o HTTPS estándar con certificados de cliente.

El administrador puede actualizar, reinicializar, reiniciar o resincronizar los teléfonos mediante la interfaz de usuario web del teléfono. El administrador también puede realizar esas tareas mediante un mensaje de notificación SIP.

Los perfiles de configuración se generan mediante herramientas comunes y de código abierto que se integran con sistemas de aprovisionamiento de proveedor de servicios.

Temas relacionados

Permitir y configurar actualizaciones del perfil, en la página 38

Permitir y configurar actualizaciones del perfil

Se permiten las actualizaciones del perfil en los intervalos especificados. Los perfiles actualizados se envían desde un servidor al teléfono mediante TFTP, HTTP o HTTPS.

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Seleccione **Voz** > **Aprovisionamiento**.

Paso 2 En la sección **Perfil de configuración**, elija **Sí** en el cuadro de lista desplegable **Activación de aprovisionamiento**.

Paso 3 Introduzca los parámetros.

Paso 4 Haga clic en **Enviar todos los cambios**.

Temas relacionados

Actualizaciones de perfil y actualizaciones de firmware, en la página 37

Permitir y configurar actualizaciones de Firmware

Se permiten las actualizaciones de firmware en los intervalos especificados. El firmware actualizado se envía desde un servidor al teléfono mediante TFTP o HTTP. La seguridad no es un problema con una actualización del firmware, debido a que el firmware no contiene información personal.

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Seleccione **Voz** > **Aprovisionamiento**.

Paso 2 En la sección **Actualización de firmware**, elija **Sí** en el cuadro de lista desplegable **Activar actualización**.

Paso 3 Introduzca los parámetros.

Paso 4 Haga clic en **Enviar todos los cambios**.

Actualización de firmware mediante TFTP, HTTP o HTTPS

El teléfono admite la actualización con una sola imagen mediante TFTP, HTTP o HTTPS.

Nota Es posible que el retorno a versiones anteriores no esté disponible para todos los dispositivos. Para obtener más información, consulte las notas de versión para su teléfono y la versión de firmware.

Antes de empezar

El archivo de carga de firmware debe descargarse de un servidor accesible.

Procedimiento

Paso 1 Cambie el nombre de la imagen de la siguiente manera:

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

donde:

`x8xx` es la serie del teléfono, como 6841.

`aa-b-c` es el número de versión, por ejemplo, 10-4-1

Paso 2 Utilice el comando **`tar -xzvf`** para descomprimir el archivo tarball.

Paso 3 Copie la carpeta al directorio de descarga TFTP, HTTP o HTTPS.

Paso 4 Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Paso 5 Seleccione **Voz** > **Aprovisionamiento**.

Paso 6 Busque el nombre de archivo de carga que termina en **.loads** y agréguelo a la dirección URL válida.

Paso 7 Haga clic en **Enviar todos los cambios**.

Actualizar el firmware con un comando de explorador

Se puede usar un comando de actualización introducido en la barra de direcciones del navegador para actualizar el firmware del teléfono. El teléfono solo se actualiza cuando está inactivo. La actualización se intenta automáticamente tras completar la llamada.

Procedimiento

Para actualizar el teléfono con una dirección URL en un explorador web, introduzca este comando:

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

CAPÍTULO 3

Aprovisionamiento previo interno y aprovisionamiento de servidores

Aprovisionamiento previo interno y aprovisionamiento de servidores

El proveedor de servicios realiza un aprovisionamiento previo de teléfonos, distintos de las unidades RC, con un perfil. El perfil de aprovisionamiento previo puede contener un conjunto limitado de parámetros que resincronizan el teléfono. El perfil también puede incluir un conjunto completo de parámetros proporcionados por el servidor remoto. De forma predeterminada, el teléfono se resincroniza al encender el sistema y a los intervalos configurados en el perfil. Cuando el usuario se conecta el teléfono en las instalaciones del cliente, el dispositivo descarga el perfil actualizado y cualquier actualización de firmware.

Este proceso de aprovisionamiento previo, implementación y aprovisionamiento remoto puede realizarse de varias maneras.

Preparación de servidor y las herramientas de software

Los ejemplos de este capítulo requieren la disponibilidad de uno o varios servidores. Estos servidores pueden instalarse y ejecutarse en un equipo local:

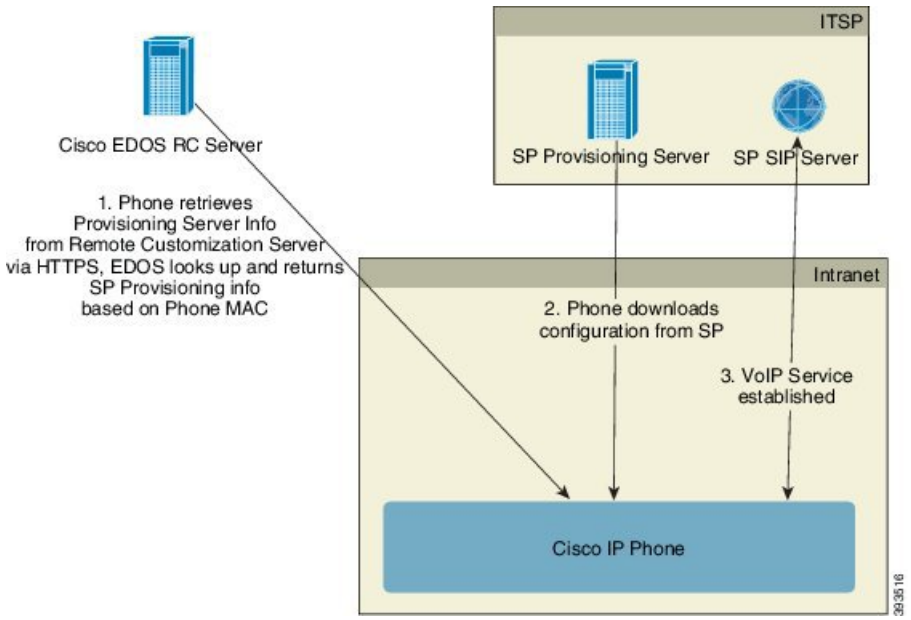
- TFTP (puerto UDP 69)
- syslog (puerto UDP 514)
- HTTP (puerto TCP 80)
- HTTPS (puerto TCP 443).

Para solucionar problemas de configuración del servidor, resulta útil instalar clientes para cada tipo de servidor en un servidor independiente. Esta práctica establece el funcionamiento correcto del servidor, independientemente de la interacción con los teléfonos.

También le recomendamos que instale estas herramientas de software:

- Para generar los perfiles de configuración, instale la utilidad de compresión gzip de código abierto.
- Para el cifrado de perfil y las operaciones de HTTPS, instale el paquete de software de código abierto OpenSSL.
- Para probar la generación de perfil dinámica y en aprovisionamiento remoto en un solo paso mediante HTTPS, se recomienda un idioma de secuencias de comandos con compatibilidad con secuencias de comandos CGI. Las herramientas de lenguaje Perl de código abierto son un ejemplo de lenguaje de secuencias de comandos.
- Para verificar los intercambios seguros entre los servidores de aprovisionamiento y los teléfonos, instale un rastreador de paquetes Ethernet (por ejemplo, Ethereal/Wireshark, de descarga gratuita). Capturar un seguimiento de paquetes de Ethernet de la interacción entre el teléfono y el servidor de aprovisionamiento. Para ello, ejecute el rastreador de paquetes en un equipo que esté conectado a un conmutador con la duplicación de puertos activada. Para las transacciones HTTPS, puede utilizar la utilidad ssldump.

Distribución de Personalización remota (RC)



Todos los teléfonos se ponen en contacto con el servidor Cisco EDOS RC hasta que se aprovisionan inicialmente.

En un modelo de distribución RC, un cliente adquiere un teléfono que ya se ha asociado con un proveedor de servicio específico en el servidor Cisco EDOS RC. El proveedor de servicio de telefonía de Internet (ITSP) configura y mantiene un servidor de aprovisionamiento y registra su información del servidor de aprovisionamiento en el servidor Cisco EDOS RC.

Cuando se enciende el teléfono con una conexión a Internet, el estado de personalización para el teléfono sin aprovisionar es **Abierto**. En primer lugar, el teléfono solicita al servidor DHCP local el aprovisionamiento de información del servidor y establece el estado de personalización del teléfono. Si la consulta DHCP es correcta, el estado de personalización se establece en **Anulado** y no se intenta el proceso RC porque DHCP proporciona la información de servidor de aprovisionamiento necesaria.

Cuando un teléfono se conecta a una red por primera vez o después de un restablecimiento de los valores de fábrica, si no hay ninguna configuración de opciones de DHCP, se pone en contacto con un servidor de activación de dispositivos para un aprovisionamiento sin necesidad de ninguna intervención. Los nuevos teléfonos utilizarán «activate.cisco.com» en lugar de «webapps.cisco.com» para el aprovisionamiento. Los teléfonos con la versión de firmware anterior a 11.2(1) seguirán usando webapps.cisco.com. Cisco recomienda permitir que los nombres de dominio atraviesen el firewall.

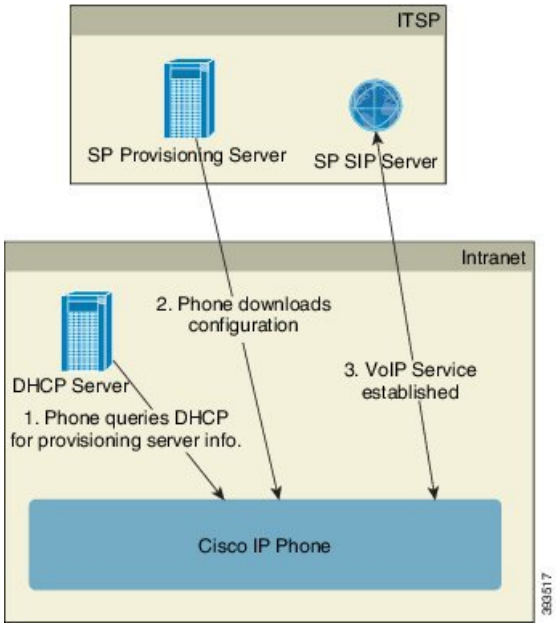
Si el servidor DHCP no proporciona la información del servidor de aprovisionamiento, el teléfono consulta con el servidor Cisco EDOS RC y proporciona su dirección MAC y el modelo, y el estado de personalización se establece en **Pendiente**. El servidor Cisco EDOS responde con la información del servidor de aprovisionamiento del proveedor de servicios asociado, incluyendo la dirección URL del servidor y el estado de personalización del teléfono se establece como **Personalización pendiente**. A continuación, el teléfono ejecuta un comando URL de resincronización para recuperar la configuración del proveedor de servicios y, si tiene éxito, el estado de personalización se ajusta en **Adquirido**.

Si el servidor Cisco EDOS RC no tiene un proveedor de servicios asociado con el teléfono, el estado de personalización del teléfono se ajusta en **No disponible**. El teléfono se puede configurar manualmente o se puede agregar una asociación para el proveedor de servicios del teléfono en el servidor Cisco EDOS.

Si un teléfono se aprovisiona mediante LCD o la utilidad de configuración web, antes de que el estado de personalización se convierta en **Adquirido**, se ajusta en **Anulado** y no se realizarán consultas en el servidor Cisco EDOS a menos que el teléfono se restablezca a los valores de fábrica.

Cuando el teléfono se haya aprovisionado, el servidor Cisco EDOS RC no se utiliza a menos que el teléfono se restablezca a los valores de fábrica.

Aprovisionamiento previo de un dispositivo interno



Con la configuración predeterminada de fábrica de Cisco, el teléfono intenta automáticamente resincronizar con un perfil en un servidor TFTP. Un servidor DHCP administrado en una LAN proporciona la información sobre el perfil y el servidor TFTP que se configura para el aprovisionamiento previo en el dispositivo. El proveedor de servicios conecta cada teléfono nuevo a la red LAN. El teléfono resincroniza con el servidor TFTP local automáticamente e inicializa su estado interno como preparación para la implementación. Este perfil de aprovisionamiento previo normalmente incluye la dirección URL de un servidor de aprovisionamiento remoto. El servidor de aprovisionamiento mantiene el dispositivo actualizado después de su implementación y conectado a la red de cliente.

Se puede escanear el código de barras del dispositivo aprovisionado previamente para registrar su dirección MAC o su número de serie antes de que el teléfono se envíe al cliente. Esta información puede utilizarse para crear el perfil con el que el teléfono se resincroniza.

Tras recibir el teléfono, el cliente lo conecta con el enlace de banda ancha. Al encenderlo, el teléfono se pone en contacto con el servidor de aprovisionamiento a través de la dirección URL que se configura mediante el aprovisionamiento previo. Por tanto, el teléfono puede resincronizar y actualizar el perfil y el firmware según sea necesario.

Temas relacionados

Distribución comercial, en la página 6
Aprovisionamiento de TFTP, en la página 45

Configuración del servidor de aprovisionamiento

En esta sección se describen los requisitos de configuración para el aprovisionamiento de un teléfono mediante varios servidores y diferentes situaciones. Para los propósitos de este documento y para realizar pruebas, los

servidores de aprovisionamiento se instalan y se ejecutan en un equipo local. Además, las herramientas de software disponibles de forma general son útiles para el aprovisionamiento de los teléfonos.

Aprovisionamiento de TFTP

Los teléfonos admiten TFTP para la resincronización de aprovisionamiento y las operaciones de actualización de firmware. Cuando los dispositivos se implementen de forma remota, se recomienda HTTPS, pero también se puede usar HTTP y TFTP. Para ello se necesita el cifrado del archivo de aprovisionamiento para agregar seguridad, ya que ofrece mayor fiabilidad, dados los mecanismos de protección de NAT y del router. TFTP es útil para el aprovisionamiento previo interno de un gran número de dispositivos suministrados.

El teléfono puede obtener una dirección IP de un servidor TFTP directamente desde el servidor DHCP a través de la opción de DHCP 66. Si se configura Profile_Rule con la ruta del archivo de ese servidor TFTP, el dispositivo descarga su perfil desde el servidor TFTP. La descarga se produce cuando el dispositivo está conectado a una LAN y se enciende.

La regla Profile_Rule proporcionada con la configuración predeterminada de fábrica es *&PN*.cfg, donde *&PN* representa el nombre del modelo de teléfono.

Por ejemplo, para CP-6841-3PCC, el nombre de archivo es CP-6841-3PCC.cfg.

Para un dispositivo con el perfil predeterminado de fábrica, durante el encendido, el dispositivo resincroniza con este archivo en el servidor TFTP local que la opción 66 de DHCP especifica. La ruta del archivo es relativa al directorio raíz virtual del servidor TFTP.

Temas relacionados

Aprovisionamiento previo de un dispositivo interno, en la página 44

NAT y Control de punto final remoto

El teléfono es compatible con la traducción de direcciones de red (NAT) para acceder a Internet a través de un router. Para mejorar la seguridad, el router puede intentar bloquear paquetes entrantes no autorizados mediante la implementación de NAT simétrica, una estrategia de filtrado de paquetes con restricciones estrictas para los paquetes que pueden entrar en la red protegida desde Internet. Por este motivo, no se recomienda el aprovisionamiento remoto mediante el uso de TFTP.

VoIP IP puede coexistir con NAT solo cuando se proporciona algún tipo de NAT transversal. Configure el cruce sencillo de UDP a través de NAT (STUN). Esta opción requiere que el usuario tenga:

- Una dirección IP dinámica externa (pública) IP de su servicio
- Un equipo que ejecute el software de servidor STUN
- Un dispositivo de borde con un mecanismo NAT asimétrico

Aprovisionamiento de HTTP

El teléfono se comporta igual que un navegador que solicita páginas web de un sitio remoto de Internet. Esto proporciona un medio fiable de alcanzar el servidor de aprovisionamiento, incluso cuando un router del cliente implementa NAT simétrica u otros mecanismos de protección. HTTP y HTTPS funcionan de forma más fiable que TFTP en las implementaciones remotas, especialmente cuando se conectan las unidades implementadas detrás de cortafuegos residenciales o routers con capacidad NAT. HTTP y HTTP son intercambiables en las descripciones siguientes de tipo de solicitud.

El aprovisionamiento basado en HTTP depende del método GET de HTTP para recuperar los perfiles de configuración. Normalmente, se crea un archivo de configuración para cada teléfono implementado y estos archivos se almacenan en un directorio de servidor HTTP. Cuando el servidor recibe la solicitud GET, simplemente devuelve el archivo que se especifica en el encabezado de la solicitud GET.

En lugar de un perfil estático el perfil de configuración se puede generar dinámicamente consultando una base de datos de cliente y generando el perfil sobre la marcha.

Cuando el teléfono solicita una resincronización, puede utilizar el método POST de HTTP para solicitar los datos de configuración de resincronización. El dispositivo puede configurarse para transmitir cierta información de estado e identificación al servidor en el cuerpo de la solicitud POST de HTTP. El servidor utiliza esta información para generar un perfil de configuración de la respuesta deseada o para almacenar la información de estado para su posterior análisis y el seguimiento.

Como parte de las solicitudes GET y POST, el teléfono incluye automáticamente información de identificación básica en el campo de agente de usuario del encabezado de solicitud. Esta información incluye el fabricante, el nombre del producto, la versión de firmware actual y el número de serie del dispositivo.

En el ejemplo siguiente es el campo de solicitud de agente de usuario de CP-6841-3PCC:

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

Cuando el teléfono se configura para resincronizar con un perfil de configuración mediante el protocolo HTTP, se recomienda utilizar HTTPS o que se cifre el perfil para proteger la información confidencial. Los perfiles cifrados que el teléfono descarga mediante el protocolo HTTP evitan el riesgo de exposición de información confidencial que se incluye en el perfil de configuración. Este modo de resincronización genera una carga de cálculo menor en el servidor de aprovisionamiento en comparación con el uso de HTTPS.

El teléfono puede descifrar perfiles de cifrado con uno de estos métodos de cifrado:

- Cifrado AES-256-CBC
- Cifrado basado en RFC-8188 cifrado con cifrado AES-128-GCM

Nota Los teléfonos son compatibles con HTTP Versión 1.0, HTTP Versión 1.1 y codificación por fragmentos cuando HTTP Versión 1.1 es el protocolo de transporte negociado.

Gestión de código de estado HTTP en la resincronización y actualización

El teléfono admite la respuesta HTTP para el aprovisionamiento remoto (resincronización). El comportamiento actual del teléfono se divide en tres formas:

- A: Éxito, cuando los valores de "Resincronización periódica" y "Retraso aleatorio de resincronización" determinan las solicitudes posteriores.
- B: error si no encuentra el archivo o el perfil está dañado. El valor "Retraso de reintento por error de resincronización" determina las solicitudes posteriores.
- C: otro fallo cuando una URL o una dirección IP incorrecta causa un error de conexión. El valor "Retraso de reintento por error de resincronización" determina las solicitudes posteriores.

Tabla 2: Comportamiento del teléfono para las respuestas HTTP

Código de estado HTTP	Descripción	Comportamiento del teléfono
301 movido permanentemente	Esta solicitud y las futuras solicitudes deben dirigirse a una nueva ubicación.	Reintentar la solicitud de forma inmediata con la nueva ubicación.
302 Encontrado	Se conoce como Movido temporalmente.	Reintentar la solicitud de forma inmediata con la nueva ubicación.
3xx	Otras respuestas 3xx no procesadas.	C
400 Solicitud errónea	La solicitud no puede cumplirse debido a sintaxis incorrecta.	C
401 No autorizado	Desafío de autenticación de acceso resumido o básico.	Reintentar inmediatamente la solicitud con credenciales de autenticación. Máximo de 2 reintentos. En caso de error, el comportamiento del teléfono es C.
403 Prohibido	El servidor no responde.	C
404 No encontrado	No se encuentra un recurso solicitado. Las solicitudes posteriores al cliente están permitidas.	B
407 Se necesita autenticación de proxy	Desafío de autenticación de acceso resumido o básico.	Reintentar inmediatamente la solicitud con credenciales de autenticación. Número máximo de dos reintentos. En caso de error, el comportamiento del teléfono es C.
4xx	No se procesan de otros códigos de estado de error del cliente.	C
500 Error interno del servidor	Mensaje de error genérico.	El comportamiento del teléfono es C.
501 No implementado	El servidor no reconoce el método de solicitud o no tiene la capacidad para cumplir con la solicitud.	El comportamiento del teléfono es C.
502 Gateway erróneo	El servidor actúa como una puerta de enlace o proxy y recibe una respuesta no válida desde el servidor ascendente.	El comportamiento del teléfono es C.
503 Servicio no disponible	El servidor no está disponible (sobrecarga o inactivo por razones de mantenimiento). Este es un estado temporal.	El comportamiento del teléfono es C.

Código de estado HTTP	Descripción	Comportamiento del teléfono
504 Tiempo de espera de gateway agotado	El servidor actúa como una puerta de enlace o proxy y no recibe una respuesta desde el servidor ascendente dentro del plazo de tiempo.	C
5xx	Otro error de servidor	C

Aprovisionamiento HTTPS

El teléfono admite HTTPS para aprovisionamiento con el fin de aumentar la seguridad de la gestión de unidades implementadas de forma remota. Cada teléfono lleva a un único certificado de cliente SSL (y una clave privada asociada), además de un certificado raíz del servidor de la entidad emisora de certificados Sipura. El último permite al teléfono reconocer los servidores de aprovisionamiento autorizados y los servidores no autorizados se rechazan. Por otro lado, el certificado de cliente permite que el servidor de aprovisionamiento identifique el dispositivo individual que emite la solicitud.

Para que un proveedor de servicios administre la implementación mediante HTTPS, se debe generar un certificado de servidor para cada servidor de aprovisionamiento con el que el teléfono se resincroniza mediante HTTPS. El certificado de servidor debe estar firmado por la clave de raíz de la entidad emisora de certificados del servidor de Cisco, cuyo certificado se lleva a cabo por todas las unidades implementadas. Para obtener un certificado de servidor firmado, el proveedor de servicios debe reenviar una solicitud de firma de certificado a Cisco, que firma y devuelve el certificado de servidor para la instalación en el servidor de aprovisionamiento.

El certificado del servidor de aprovisionamiento debe contener el campo Nombre común (CN) y el FQDN del host que ejecuta el servidor en el asunto. Opcionalmente, puede contener la información de FQDN del host, separado por un carácter de barra diagonal (/). Los ejemplos siguientes son de entradas CN que el teléfono ha aceptado como válidas:

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

Además de comprobar el certificado del servidor, el teléfono prueba la dirección IP del servidor con una búsqueda DNS del nombre del servidor especificado en el certificado de servidor.

Obtención de un certificado de servidor firmado

La utilidad OpenSSL puede generar una solicitud de firma del certificado. El ejemplo siguiente muestra el comando **openssl** que genera un par de claves pública/privada de 1024 bits RSA y una solicitud de firma de certificado:

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

Este comando genera la clave privada del servidor en **privkey.pem** y una solicitud de firma del certificado correspondiente en **provserver.csr**. El proveedor de servicios mantiene **privkey.pem** en secreto y envía **provserver.csr** a Cisco utiliza para la firma. Tras recibir el archivo **provserver.csr**, Cisco genera **provserver.crt**, el certificado de servidor firmado.

Procedimiento

Paso 1 Vaya a https://software.cisco.com/software/cda/home e inicie sesión con sus credenciales de CCO.

Nota Cuando un teléfono se conecta a una red por primera vez o después de un restablecimiento de los valores de fábrica y no hay ninguna configuración de opciones de DHCP, se pone en contacto con un servidor de activación de dispositivos para un aprovisionamiento sin necesidad de ninguna intervención. Los nuevos teléfonos utilizan «activate.cisco.com» en lugar de «webapps.cisco.com» para el aprovisionamiento. Los teléfonos con la versión de firmware anterior a 11.2(1) siguen usando «webapps.cisco.com». Recomendamos permitir que los nombres de dominio atraviesen el firewall.

Paso 2 Seleccione **Administración de certificados**.

En la ficha **Firmar CSR**, el archivo CSR del paso anterior se carga para la firma.

Paso 3 Desde el cuadro de la lista desplegable **Seleccionar producto**, seleccione **SPA1xx firmware 1.3.3 y el firmware más reciente/SPA232D 1.3.3, el firmware más reciente/SPA5xx 7.5.6 y el firmware más reciente/CP-78xx-3PCC/CP-88xx-3PCC**.

Nota Este producto incluye los teléfonos multiplataforma Cisco IP Phone serie 6800.

Paso 4 En el campo **Archivo CSR**, haga clic en **Examinar** y seleccione el archivo CSR para la firma.

Paso 5 Seleccione el método de cifrado:

- MD5
- SHA1
- SHA256

Cisco recomienda que seleccione el cifrado SHA256.

Paso 6 En el cuadro de la lista desplegable **Duración del inicio de sesión**, seleccione la duración aplicable (por ejemplo, 1 año).

Paso 7 Haga clic en **Firmar solicitud de certificado**.

Paso 8 Seleccione una de las siguientes opciones para recibir el certificado firmado:

- **Introduzca la dirección de correo electrónico del destinatario**: si desea recibir el certificado por correo electrónico, introduzca su dirección de correo electrónico en este campo.
- **Descarga**: si desea que se descargue el certificado firmado, seleccione esta opción.

Paso 9 Haga clic en **Enviar**.

El certificado de servidor firmado se envía a la dirección de correo electrónico proporcionada o se descarga.

Certificado raíz de cliente de CA de teléfono multiplataforma

Cisco también proporciona un certificado raíz de cliente de teléfono multiplataforma al proveedor de servicios. Este certificado raíz certifica la autenticidad del cliente de certificado que cada teléfono lleva. Los teléfonos multiplataforma también admiten certificados firmados de terceros como los proporcionados por Verisign, Cybertrust, etc.

El certificado del cliente exclusivo que cada dispositivo ofrece durante una sesión HTTPS contiene información de identificación incrustada en el campo de asunto. Esta información se puede poner a disposición, mediante

el servidor HTTPS, de una secuencia de comandos CGI para manejar solicitudes seguras. En particular, el asunto del certificado indica el nombre del producto de la unidad (elemento OU), la dirección MAC (elemento S) y el número de serie (elemento L).

El ejemplo siguiente del campo de asunto del certificado de cliente de teléfonos multiplataforma Cisco IP Phone 6841 muestra estos elementos:

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

Para determinar si un teléfono contiene un certificado individualizado, utilice la variable de marco de aprovisionamiento $CCERT. El valor de variable se expandirá a Instalado o No instalado, de acuerdo con la presencia o la ausencia de un certificado exclusivo del cliente. En el caso de un certificado genérico, se puede obtener el número de serie de la unidad del encabezado de la solicitud HTTP en el campo de agente de usuario.

Los servidores HTTPS pueden configurarse para solicitar certificados SSL de los clientes que se conectan. Si se activa, el servidor puede utilizar el certificado raíz de cliente de teléfono multiplataforma proporcionado por Cisco para verificar el certificado del cliente. A continuación, el servidor puede proporcionar la información del certificado a un CGI para su procesamiento posterior.

La ubicación de almacenamiento de certificados puede variar. Por ejemplo, en una instalación Apache, las rutas de archivo de almacenamiento del certificado firmado por el servidor de aprovisionamiento tienen asociados una clave privada y el certificado raíz de cliente de entidad emisora de certificados de teléfono multiplataforma de la siguiente manera:

```
# 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 obtener información específica, consulte la documentación de un servidor HTTPS.

La autoridad de raíz de certificado de cliente de Cisco inicia cada certificado exclusivo. El certificado raíz correspondiente estará disponible para los proveedores de servicios para finalidades de autenticación del cliente.

Servidores de aprovisionamiento redundantes

El servidor de aprovisionamiento se puede especificar como una dirección IP o como un nombre de dominio completo (FQDN). El uso de un FQDN facilita la implementación de servidores de aprovisionamiento redundantes. Cuando se identifica el servidor de aprovisionamiento a través de un nombre de dominio completo, el teléfono intenta resolver el FQDN en una dirección IP a través de DNS. Solo se admiten los registros A de DNS para el aprovisionamiento; la resolución de dirección SRV DNS no está disponible para el aprovisionamiento. El teléfono continúa procesando registros A hasta que un servidor responde. Si no hay ningún servidor asociado con las respuestas de registros A, el teléfono registra un error en el servidor Syslog.

Servidor syslog

Si se configura un servidor Syslog en el teléfono mediante el uso de los parámetros de <Syslog Server>, las operaciones de resincronización y actualización envían mensajes al servidor Syslog. Se puede generar un

mensaje al principio de la solicitud de un archivo remoto (perfil de configuración o carga de firmware) y a la conclusión de la operación (indicando el éxito o el fracaso).

Los mensajes registrados se configuran en los siguientes parámetros y las macros se expanden en los mensajes de syslog reales:

- Log_Request_Msg (Mensaje de solicitud de registro)
- Log_Success_Msg (Mensaje de registro correcto)
- Log_Failure_Msg (Mensaje de error de registro)

CAPÍTULO 4

Ejemplos de aprovisionamiento

Descripción general de ejemplos de aprovisionamiento

En este capítulo se proporcionan procedimientos de ejemplo para transferir perfiles de configuración entre el teléfono y el servidor de aprovisionamiento.

Para obtener más información sobre la creación de perfiles de configuración, consulte Formatos de aprovisionamiento, en la página 15.

Resincronización básica

En esta sección se muestra la funcionalidad de resincronización básica de los teléfonos.

Resincronización TFTP

El teléfono admite varios protocolos de red para recuperar los perfiles de configuración. El protocolo de transferencia de perfil más básico es TFTP (RFC1350). TFTP se utiliza de forma generalizada para el aprovisionamiento de los dispositivos de red dentro de las redes LAN privadas. Aunque no se recomienda para la implementación de terminales remotos a través de Internet, TFTP puede ser adecuado para la implementación dentro de las organizaciones pequeñas, para el aprovisionamiento previo interno y para el desarrollo y las pruebas. Consulte Aprovisionamiento previo de un dispositivo interno, en la página 44 para obtener más información sobre el aprovisionamiento previo. En el procedimiento siguiente, se modifica un perfil después de descargar un archivo desde un servidor TFTP.

Procedimiento

Paso 1 En un entorno de LAN, conecte un PC y un teléfono a un concentrador, un conmutador o un router pequeño.

Paso 2 En el PC, instale y active un servidor TFTP.

Paso 3 Use un editor de texto para crear un perfil de configuración que establezca el valor de GPP_A en 12345678, como se muestra en el ejemplo.

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

Paso 4 Guarde el perfil con el nombre `basic.txt` en el directorio raíz del servidor TFTP.

Puede comprobar que el servidor TFTP está configurado correctamente: solicite el archivo `basic.txt` utilizando un cliente TFTP distinto del teléfono. Es preferible utilizar a un cliente TFTP que se ejecute en un host independiente del servidor de aprovisionamiento.

Paso 5 Abra el explorador web del PC en la página de administración/configuración avanzada. Por ejemplo, si la dirección IP del teléfono es 192.168.1.100:

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

Paso 6 Seleccione la ficha **Voz** > **Aprovisionamiento** e inspeccione los valores de los parámetros generales de GPP_A a GPP_P. Deben estar vacíos.

Paso 7 Resincronice el teléfono de prueba con el perfil de configuración `basic.txt` abriendo la dirección URL de configuración en la ventana de un explorador web.

Si la dirección IP del servidor TFTP es 192.168.1.200, el comando debe ser similar al siguiente ejemplo:

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

Cuando el teléfono reciba este comando, el dispositivo en la dirección 192.168.1.100 solicita el archivo `basic.txt` desde el servidor TFTP en la dirección IP 192.168.1.200. A continuación, el teléfono analiza el archivo descargado y actualiza el parámetro GPP_A con el valor 12345678.

Paso 8 Compruebe que el parámetro se haya actualizado correctamente: actualice la página de configuración en el explorador web de PC y seleccione la ficha **Voz** > **Aprovisionamiento**.

El parámetro GPP_A ahora debe contener el valor 12345678.

Uso de Syslog para registrar mensajes

El teléfono envía un mensaje de Syslog al servidor de Syslog designado cuando el dispositivo está a punto para resincronizar con un servidor de aprovisionamiento y después de que la resincronización se haya completado o ha fallado. Para identificar este servidor, puede acceder a la página web de administración del teléfono (consulte Acceso a la página web del teléfono, en la página 9), seleccione **Voz** > **Sistema** e identifique el servidor en el parámetro **Servidor Syslog** de la sección **Optional Network Configuration** (Configuración de red opcional). Configure la dirección IP del servidor syslog en el dispositivo y observe los mensajes que se generan durante los procedimientos restantes.

Procedimiento

Paso 1 Instale y active un servidor syslog en el PC local.

Paso 2 Programe la dirección IP del PC en el parámetro Syslog_Server del perfil y envíe el cambio:

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

Paso 3 Haga clic en la ficha **Sistema** e introduzca el valor de su servidor syslog local en el parámetro Syslog_Server.

Paso 4 Repita la operación de resincronización tal y como se describe en Resincronización TFTP, en la página 53.

El dispositivo genera dos mensajes de syslog durante la resincronización. El primer mensaje indica que una solicitud está en curso. El segundo mensaje marca como correcta o errónea la resincronización.

Paso 5 Compruebe que el servidor syslog haya recibido mensajes similares a los siguientes:

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

Los mensajes detallados están disponibles mediante la programación de un parámetro Debug_Server (en lugar del parámetro Syslog_Server) con la dirección IP del servidor syslog y estableciendo Debug_Level en un valor entre 0 y 3 (3 es más detallado):

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

El contenido de estos mensajes se puede configurar mediante los parámetros siguientes:

- Log_Request_Msg (Mensaje de solicitud de registro)
- Log_Success_Msg (Mensaje de registro correcto)
- Log_Failure_Msg (Mensaje de error de registro)

Si alguno de estos parámetros está desactivado, no se genera el mensaje de Syslog correspondiente.

Resincronización automática de un dispositivo

Un dispositivo puede resincronizarse periódicamente con el servidor de aprovisionamiento para asegurarse de que todos los cambios de perfil realizados en el servidor se propagan al dispositivo de punto final (en lugar de enviar una solicitud de resincronización explícita a los puntos finales).

Para hacer que el teléfono se resincronice periódicamente con un servidor, se define una dirección URL de perfil de configuración mediante el parámetro Profile_Rule y se define un período de resincronización mediante el parámetro Resync_Periodic.

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Seleccione **Voz** > **Aprovisionamiento**.

Paso 2 Defina el parámetro Profile_Rule. En este ejemplo se supone una dirección IP del servidor TFTP de 192.168.1.200.

Paso 3 En el campo **Resincronización periódica**, introduzca un valor pequeño para realizar pruebas, por ejemplo, **30** segundos.

Paso 4 Haga clic en **Submit all Changes** (Enviar todos los cambios).

Con la nueva configuración de parámetro, el teléfono se resincroniza dos veces por minuto con los archivos de configuración que la dirección URL especifica.

Paso 5 Tenga en cuenta los mensajes que resulten de seguimiento de syslog (tal y como se describe en la sección Uso de Syslog para registrar mensajes, en la página 54).

Paso 6 Asegúrese de que el campo **Resincronizar al restablecer** esté establecido como **Sí**.

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

Paso 7 Apague y encienda el teléfono para forzar la resincronización con el servidor de aprovisionamiento.

Si la operación de resincronización falla por cualquier motivo, por ejemplo, si el servidor no responde, la unidad espera (durante el número de segundos que se configura en **Resync Error Retry Delay** (Retraso de reintento por error de resincronización)) antes de intentar la resincronización de nuevo. Si **Resync Error Retry Delay** (Retraso de reintento por error de resincronización) es cero, el teléfono no intenta resincronizar tras un intento de resincronización fallido.

Paso 8 (Opcional) Establezca el valor del campo **Retraso de reintento por error de resincronización** en un número pequeño, por ejemplo, **30**.

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

Paso 9 Desactive el servidor TFTP y observe los resultados de la salida de syslog.

Perfiles únicos, expansión de macro y HTTP

En una implementación donde cada teléfono se debe configurar con valores distintos para algunos parámetros, por ejemplo, User_ID (Id. de usuario) o Display_Name (Nombre para mostrar), el proveedor de servicios puede crear un perfil exclusivo para cada dispositivo implementado y alojar dichos perfiles en un servidor de aprovisionamiento. Cada teléfono, a su vez, debe estar configurado para resincronizar con su propio perfil según una convención de nombres de perfil predeterminada.

La sintaxis de la dirección URL de perfil puede incluir información de identificación específica de cada teléfono, como la dirección MAC o número de serie, utilizando la expansión de macro de variables integradas. La expansión de macro elimina la necesidad de especificar estos valores en distintas ubicaciones dentro de cada perfil.

Una regla de perfil experimenta una expansión de macro antes de que la regla se aplique al teléfono. La expansión de macro controla varios valores, por ejemplo:

- $MA expandirá la dirección MAC de 12 dígitos de la unidad (con dígitos hexadecimales en minúsculas). Por ejemplo, 000e08abcdef.
- $SN se expande al número de serie de la unidad. Por ejemplo, 88012BA01234.

Otros valores se pueden expandir mediante macro de este modo, incluidos todos los parámetros de propósito general, de GPP_A a GPP_P. Se puede ver un ejemplo de este proceso en la sección Resincronización TFTP, en la página 53. La expansión de macro no se limita al nombre de archivo de la dirección URL, pero también se pueden aplicar a cualquier parte de los parámetros de regla de perfil. Estos parámetros se indican como $A a $P. Para obtener una lista completa de variables que están disponibles para que la expansión de macro, consulte Variables de expansión de macro, en la página 78.

En este ejercicio, se aprovisiona un perfil específico a un teléfono en un servidor TFTP.

Ejercicio: aprovisionamiento de un perfil específico de un teléfono IP en un servidor TFTP

Procedimiento

Paso 1 Obtenga la dirección MAC del teléfono de la etiqueta del producto. (La dirección MAC es el número, con números y dígitos hexadecimales en minúsculas, como por ejemplo, 000e08aabbcc.

Paso 2 Copie el archivo de configuración `basic.txt` (descrito en la sección Resincronización TFTP, en la página 53) en un nuevo archivo con el nombre `CP-xxxx-3PCC direcciónmac.cfg` (sustituyendo `xxxx` por el número de modelo y `direcciónmac` por la dirección MAC del teléfono).

Paso 3 Mueva el archivo nuevo al directorio raíz virtual del servidor TFTP.

Paso 4 Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Paso 5 Seleccione **Voz** > **Aprovisionamiento**.

Paso 6 Introduzca `tftp://192.168.1.200/CP-6841-3PCC$MA.cfg` en el campo **Regla de perfil**.

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

Paso 7 Haga clic en **Submit All Changes** (Enviar todos los cambios). Esto provoca un reinicio inmediato y la resincronización.

Cuando se produce la siguiente resincronización, el teléfono recupera el nuevo archivo al expandir la macro de expresión $MA en su dirección MAC.

Resincronización GET de HTTP

HTTP proporciona un mecanismo de resincronización más fiable que TFTP porque HTTP establece una conexión TCP y TFTP usa UDP menos fiable. Además, los servidores HTTP ofrecen características mejoradas de filtrado y registro en comparación con los servidores TFTP.

En el lado del cliente, el teléfono no requiere cualquier configuración especial en el servidor para que pueda resincronizar mediante HTTP. La sintaxis del parámetro Profile_Rule para la utilización de HTTP con el método GET es similar a la sintaxis que se utiliza para TFTP. Si un explorador web estándar puede recuperar un perfil de su servidor HTTP, el teléfono debería poder hacerlo también.

Ejercicio: resincronización GET de HTTP

Procedimiento

Paso 1 Instale un servidor HTTP en el PC local o en otro host accesible.

El servidor Apache de código abierto se puede descargar de Internet.

Paso 2 Copie el perfil de configuración `basic.txt` (se describe en la sección Resincronización TFTP, en la página 53) en el directorio raíz virtual del servidor instalado.

Paso 3 Para comprobar la instalación de servidor adecuado y el acceso de archivo a `basic.txt`, acceda al perfil con un explorador web.

Paso 4 Modifique Profile_Rule del teléfono de prueba para que apunte al servidor HTTP en lugar del servidor TFTP, con el fin de descargar periódicamente su perfil.

Por ejemplo, si se asume que el servidor HTTP está en 192.168.1.300, introduzca el valor siguiente:

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

Paso 5 Haga clic en **Submit All Changes** (Enviar todos los cambios). Esto provoca un reinicio inmediato y la resincronización.

Paso 6 Tenga en cuenta los mensajes de Syslog que el teléfono envía. La resincronización periódica ahora debe obtener el perfil del servidor HTTP.

Paso 7 En los registros de servidor HTTP, tenga en cuenta cómo aparece la información que identifica el teléfono de prueba en el registro de agentes de usuario.

Esta información debe incluir el fabricante, el nombre del producto, la versión de firmware actual y el número de serie.

Aprovisionamiento a través de Cisco XML

Para cada uno de los teléfonos, designado como xxxx aquí, puede realizar el aprovisionamiento mediante las funciones XML de Cisco.

Puede enviar un objeto XML al teléfono mediante un paquete Notify de SIP o un HTTP Post a la interfaz CGI del teléfono: `http://IPAddressPhone/CGI/Execute`.

CP-xxxx-3PCC amplía la función Cisco XML para que admita el aprovisionamiento a través de un objeto XML:

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

Cuando el teléfono haya recibido el objeto XML, descargará el archivo de aprovisionamiento de [regla-perfil]. Esta regla utiliza macros para simplificar el desarrollo de la aplicación de los servicios XML.

Resolución de URL con expansión de macro

Los subdirectorios con varios perfiles en el servidor proporcionan un método práctico para la administración de un gran número de dispositivos implementados. La dirección URL del perfil puede contener:

- Un nombre de servidor de aprovisionamiento o una dirección IP explícita. Si el perfil identifica el servidor de aprovisionamiento por nombre, el teléfono realiza una búsqueda DNS para resolver el nombre.
- Un puerto del servidor no estándar que se especifica en la dirección URL mediante la sintaxis estándar `:puerto` tras el nombre del servidor.
- El subdirectorio del directorio raíz virtual servidor en el que está almacenado el perfil, especificado por la anotación de URL estándar y administrado por la expansión de macro.

Por ejemplo, la siguiente regla de perfil Profile_Rule solicita el archivo de perfil ($PN.cfg) en el subdirectorio `/cisco/config` del servidor, desde el servidor TFTP que se ejecuta en el host prov.telco.com que escucha una conexión en el puerto 6900:

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

Se puede identificar un perfil de cada teléfono en un parámetro de uso general, con su valor de referencia dentro de una regla de perfil común mediante la expansión de macro.

Por ejemplo, supongamos que GPP_B se define como `Dj6Lmp23Q`.

Profile_Rule tiene el valor:

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

Cuando se expanden las resincronizaciones de dispositivo y las macros, el teléfono con una dirección MAC de 000e08012345 solicita el perfil con el nombre que contiene el dispositivo de la dirección MAC en la siguiente dirección URL:

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

Resincronización HTTPS segura

Estos mecanismos están disponibles en el teléfono para resincronizar mediante un proceso de comunicación seguro:

- Resincronización HTTPS básica
- HTTPS con la autenticación de certificado de cliente
- Filtrado de cliente HTTPS y contenido dinámico

Resincronización HTTPS básica

HTTPS agrega SSL a HTTP para el aprovisionamiento remoto para que:

- El teléfono pueda autenticar el servidor de aprovisionamiento.
- El servidor de aprovisionamiento pueda autenticar el teléfono.
- La confidencialidad de la información que se intercambia entre el teléfono y el servidor de abastecimiento esté asegurada.

SSL genera e intercambia claves secretas (simétricas) para cada conexión entre el teléfono y el servidor, mediante los pares de clave pública/privada que están preinstalados en el teléfono y el servidor de aprovisionamiento.

En el lado del cliente, el teléfono no requiere cualquier configuración especial en el servidor para que pueda resincronizar mediante HTTPS. La sintaxis del parámetro Profile_Rule para la utilización de HTTPS con el método GET es similar a la sintaxis que se utiliza para HTTP o TFTP. Si un explorador web estándar puede recuperar un perfil de un servidor HTTPS, el teléfono debería poder hacerlo también.

Además de instalar en un servidor HTTPS, un certificado de servidor SSL firmado por Cisco debe estar instalado en el servidor de aprovisionamiento. Los dispositivos no pueden resincronizarse con un servidor que utiliza HTTPS a menos que el servidor proporciona un certificado de servidor firmado por Cisco. Las instrucciones para crear certificados SSL firmados para los productos de voz pueden encontrarse en https://supportforums.cisco.com/docs/DOC-9852.

Ejercicio: Resincronización HTTPS básica

Procedimiento

Paso 1 Instale un servidor HTTPS en un host cuya dirección IP sea conocida por el servidor DNS de red a través de la traducción del nombre de host normal.

El servidor Apache de código abierto puede configurarse para que funcione como un servidor HTTPS cuando se instale con el paquete de mod_ssl de código abierto.

Paso 2 Genere una solicitud de firma de certificado de servidor para el servidor. Para este paso, es posible que necesite instalar el paquete de código abierto OpenSSL o un software equivalente. Si utiliza OpenSSL, el comando para generar el archivo CSR básico es el siguiente:

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

Este comando genera un par de clave pública/privada, que se guarda en el archivo `privkey.pem`.

Paso 3 Envíe el archivo CSR (provserver.csr) a Cisco para el inicio de sesión.

Un certificado de servidor firmado se devolverá (provserver.cert) junto con un certificado raíz de cliente de entidad emisora de certificados de Sipura, spacroot.cert.

Para obtener más información, consulte https://supportforums.cisco.com/docs/DOC-9852.

Paso 4 Guarde el certificado de servidor firmado, el archivo de par de claves privado y el certificado raíz del cliente en las ubicaciones adecuadas en el servidor.

En el caso de una instalación Apache en Linux, estas ubicaciones por lo general son las siguientes:

```
# 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
```

Paso 5 Reinicie el servidor.

Paso 6 Copie el archivo de configuración `basic.txt` (se describe en la sección Resincronización TFTP, en la página 53) en el directorio raíz virtual del servidor HTTPS.

Paso 7 Compruebe el funcionamiento correcto del servidor descargando `basic.txt` del servidor HTTPS mediante un explorador estándar desde el PC local.

Paso 8 Inspeccione el certificado del servidor que proporciona el servidor.

El explorador probablemente no reconoce el certificado como válido a no ser que se haya preconfigurado para aceptar Cisco como una entidad de certificación raíz. Sin embargo, los teléfonos esperan que el certificado esté firmado de esa manera.

Modificar la regla Profile_Rule del dispositivo de prueba para que incluya una referencia al servidor HTTPS, por ejemplo:

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

En este ejemplo se supone que el nombre del servidor HTTPS es **`my.server.com`**.

Paso 9 Haga clic en **Submit All Changes** (Enviar todos los cambios).

Paso 10 Tenga en cuenta el seguimiento de Syslog que el teléfono envía.

El mensaje de syslog debe indicar que la resincronización ha obtenido el perfil del servidor HTTPS.

Paso 11 (Opcional) Use un analizador de protocolo Ethernet en la subred del teléfono para comprobar que los paquetes estén cifrados.

En este ejercicio, no se ha habilitado la validación del certificado de cliente. La conexión entre el teléfono y el servidor está cifrada. Sin embargo, la transferencia no es segura porque cualquier cliente puede conectarse al servidor y solicitar el archivo si conoce el nombre de archivo y la ubicación del directorio. Para una resincronización segura, el servidor también debe autenticar el cliente, tal y como se demuestra en el ejercicio que se describe en la sección HTTPS con la autenticación de certificado de cliente, en la página 61.

HTTPS con la autenticación de certificado de cliente

En la configuración predeterminada de fábrica, el servidor no solicita un certificado de cliente SSL de un cliente. La transferencia del perfil no es segura, ya que cualquier cliente puede conectarse al servidor y solicitar el perfil. Puede editar la configuración para activar la autenticación del cliente; el servidor requiere un certificado de cliente para autenticar el teléfono antes de aceptar una solicitud de conexión.

A causa de este requisito, la operación de resincronización no se puede probar independientemente mediante un navegador que no tiene las credenciales correctas. El intercambio de claves de SSL dentro de la conexión de HTTPS entre el teléfono de prueba y el servidor se puede observar con la utilidad ssldump. El seguimiento de la utilidad muestra la interacción entre el cliente y el servidor.

Ejercicio: HTTPS con autenticación de certificado de cliente

Procedimiento

Paso 1 Habilite la autenticación de certificado de cliente en el servidor HTTPS.

Paso 2 En Apache (v.2), establezca lo siguiente en el servidor del archivo de configuración:

```
SSLVerifyClient  require
```

Asegúrese también de que se haya almacenado spacroot.cert tal y como se muestra en el ejercicio Resincronización HTTPS básica, en la página 59.

Paso 3 Reinicie el servidor HTTPS y observe el seguimiento de syslog desde el teléfono.

Cada resincronización al servidor ahora realiza la autenticación simétrica, para que el certificado del servidor y el certificado del cliente se comprueben antes de que se transfiera el perfil.

Paso 4 Utilice ssldump para capturar una conexión de resincronización entre el teléfono y el servidor HTTPS.

Si la validación del certificado de cliente se activa correctamente en el servidor, el seguimiento de ssldump muestra el intercambio simétrico de certificados (primer del servidor al cliente y, a continuación, del cliente al servidor) antes de los paquetes cifrados que contengan el perfil.

Con la autenticación de cliente activada, solo un teléfono con una dirección MAC que coincida con un certificado de cliente válido puede solicitar el perfil del servidor de aprovisionamiento. El servidor rechaza una solicitud de un navegador normal u otro dispositivo no autorizado.

Filtrado de cliente HTTPS y contenido dinámico

Si el servidor HTTPS está configurado para solicitar un certificado de cliente, la información del certificado identifica el teléfono que realiza la resincronización y le suministra la información de configuración correcta.

El servidor HTTPS pone la información del certificado a disposición de las secuencias de comandos CGI (o programas CGI compilados) que se invocan como parte de la solicitud de resincronización. Con fines ilustrativos, este ejercicio utiliza el lenguaje de secuencias de comandos Perl de código abierto y se supone que se utiliza Apache (v.2) como servidor HTTPS.

Procedimiento

Paso 1 Instale Perl en el host que está ejecutando el servidor HTTPS.

Paso 2 Genere la secuencia de comandos de espejo Perl siguiente:

```
#!/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>";
```

Paso 3 Guarde este archivo con el nombre de archivo `reflect.pl`, con el permiso ejecutable (chmod 755 en Linux), en el directorio de secuencias de comandos CGI del servidor HTTPS.

Paso 4 Compruebe la accesibilidad de las secuencias de comandos CGI en el servidor (es decir, `/cgi-bin/...`).

Paso 5 Modifique Profile_Rule en el dispositivo de prueba para resincronizar con la secuencia de comandos de espejo, como se muestra en el ejemplo siguiente:

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

Paso 6 Haga clic en **Submit All Changes** (Enviar todos los cambios).

Paso 7 Tenga en cuenta el seguimiento de syslog para garantizar una resincronización correcta.

Paso 8 Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Paso 9 Seleccione **Voz** > **Aprovisionamiento**.

Paso 10 Compruebe que el parámetro GPP_D contenga la información que captura la secuencia de comandos.

Esta información contiene el nombre del producto, la dirección MAC y el número de serie, si el dispositivo de prueba contiene un certificado exclusivo del fabricante. La información contiene cadenas genéricas si la unidad se fabricó antes de la versión 2.0 del firmware.

Una secuencia de comandos similar puede determinar la información sobre el dispositivo de resincronización y, a continuación, proporcionar al dispositivo los valores del parámetro de configuración adecuado.

Certificados HTTPS

El teléfono proporciona una estrategia de abastecimiento segura y fiable que se basa en las solicitudes de HTTPS del dispositivo al servidor de aprovisionamiento. Se usan un certificado de servidor y un certificado para autenticar el teléfono con el servidor y el servidor con el teléfono.

Para utilizar HTTPS con el teléfono, debe generar un certificado de solicitud de firma (CSR) y enviarlo a Cisco. El teléfono genera un certificado para la instalación en el servidor de aprovisionamiento. El teléfono acepta el certificado cuando intenta establecer una conexión HTTPS con el servidor de aprovisionamiento.

Metodología HTTPS

HTTPS cifra la comunicación entre un cliente y un servidor, lo que protege el contenido del mensaje de otros dispositivos de red. El método de cifrado del cuerpo de la comunicación entre un cliente y un servidor se basa en criptografía de claves simétricas. Con la criptografía de claves simétricas, un cliente y un servidor comparten una única clave secreta a través de un canal seguro que está protegido por el cifrado de clave pública o privada.

Los mensajes cifrados con la clave secreta solo se pueden descifrar usando la misma clave. HTTPS admite una amplia gama de algoritmos de cifrado simétrico. El teléfono implementa un cifrado de 256 bits simétrico, mediante American Encryption Standard (AES), además de RC4 de 128 bits.

HTTPS también proporciona la autenticación de un servidor y un cliente que realizan una transacción segura. Esta función se asegura de que no pueda suplantar un servidor de aprovisionamiento y un cliente individual en otros dispositivos de la red. Esta capacidad es fundamental en el contexto de aprovisionamiento de punto final remoto.

La autenticación de servidor y del cliente se realiza mediante el uso de cifrado de clave pública/privada con un certificado que contiene la clave pública. El texto que se cifra mediante una clave pública se puede descifrar solo por su clave privada correspondiente (y viceversa). El teléfono es compatible con el algoritmo Rivest-Shamir-Adleman (RSA) para el cifrado de clave pública/privada.

Certificado de servidor SSL

Cada servidor de aprovisionamiento seguro emite un certificado de servidor de Capa de sockets seguros (SSL) que Cisco firma directamente. El firmware que se ejecuta en el teléfono solo reconoce como válido un certificado de Cisco. Cuando un cliente se conecta a un servidor mediante HTTPS, el servidor rechaza cualquier certificado de servidor que no esté firmado por Cisco.

Este mecanismo protege al proveedor de servicios ante un acceso no autorizado al teléfono o ante cualquier intento de suplantar al servidor de aprovisionamiento. Sin dicha protección, un intruso podría reaprovisionar el teléfono para obtener información de configuración o para utilizar un servicio VoIP diferente. Sin la clave privada que corresponde a un certificado de servidor válido, el intruso no puede establecer comunicación con un teléfono.

Obtención de un certificado de servidor

Procedimiento

Paso 1 Póngase en contacto con una persona de asistencia de Cisco para que colabore con usted en el proceso de certificado. Si no está trabajando con una persona específica de soporte técnico, envíe su solicitud por correo electrónico a ciscosb-certadmin@cisco.com.

Paso 2 Genere una clave privada que se utilizará en una CSR (solicitud de certificado de inicio de sesión). Esta tecla es privada y no es necesario proporcionarla al servicio de asistencia de Cisco. Utilice "openssl" de código abierto para generar la clave. Por ejemplo:

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

Paso 3 Genere una CSR que contenga campos que identifiquen a su organización y su ubicación. Por ejemplo:

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

Debe tener la siguiente información:

- Campo de asunto: introduzca el nombre común (CN) que debe ser un FQDN (nombre de dominio completo). Durante el protocolo de enlace de autenticación de SSL, el teléfono comprueba que el certificado que recibe sea de la máquina que lo ha presentado.
- Nombre de host del servidor: por ejemplo, provserv.domain.com.
- Dirección de correo electrónico: introduzca una dirección de correo electrónico para que el servicio de atención al cliente pueda ponerse en contacto con usted si fuera necesario. Esta dirección de correo electrónico está visible en la CSR.

Paso 4 Envíe la CSR (en formato de archivo zip) por correo electrónico a la persona de soporte de Cisco o a ciscosb-certadmin@cisco.com. El certificado está firmado por Cisco. Cisco envía el certificado para que lo instale en el sistema.

Certificado de cliente

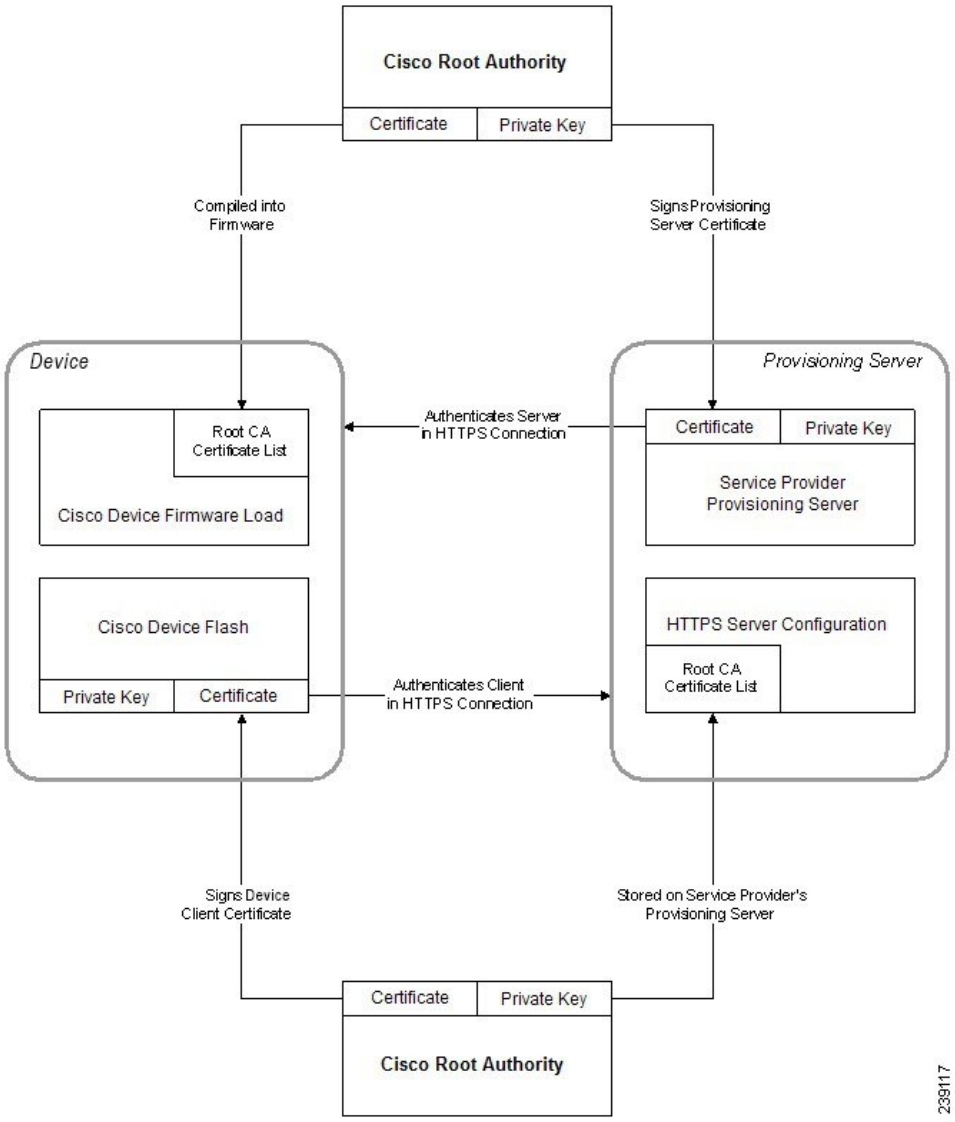
Además de un ataque directo sobre el teléfono, un intruso puede intentar ponerse en contacto con un servidor de aprovisionamiento a través de un explorador web estándar u otro cliente HTTPS para obtener el perfil de configuración del servidor de aprovisionamiento. Para evitar que este tipo de ataque, cada teléfono también incluye un certificado de cliente exclusivo, firmado por Cisco, que incluye información de identificación sobre todos los puntos finales individuales. Se asigna a cada proveedor de servicios un certificado raíz de entidad emisora de certificados capaz de autenticación de certificado del cliente de dispositivo. Esta ruta de autenticación permite que el servidor de aprovisionamiento rechace las solicitudes no autorizadas de perfiles de configuración.

Estructura de certificados

La combinación de un certificado de servidor y un certificado de cliente garantiza una comunicación segura entre un teléfono remoto y su servidor de aprovisionamiento. La ilustración siguiente muestra la relación y la ubicación de los certificados, los pares de clave pública/privada y las entidades raíz firmantes, entre el cliente de Cisco, el servidor de aprovisionamiento y la entidad emisora de certificados.

La mitad superior del diagrama muestra la autoridad raíz del servidor de aprovisionamiento que se usó para firmar el certificado de servidor de aprovisionamiento individual. El certificado raíz correspondiente se compila en el firmware, que permite al teléfono autenticar servidores de aprovisionamiento autorizados.

Figura 2: Flujo de la entidad emisora de certificados



Configuración de una entidad emisora de certificados personalizada

Se pueden usar los certificados digitales para autenticar dispositivos de red y usuarios de la red. Se pueden utilizar para negociar sesiones IPSec entre los nodos de red.

Un tercero usa una entidad emisora de certificados para validar y autenticar dos o más nodos que están intentando comunicarse. Cada nodo tiene una clave pública y privada. La clave pública cifra los datos. La clave privada descifra los datos. Como los nodos han obtenido sus certificados desde el mismo origen, se garantizan sus respectivas identidades.

El dispositivo puede utilizar los certificados digitales proporcionados por una entidad emisora de certificados (CA) externa para autenticar las conexiones IPSec.

Los teléfonos admiten un conjunto de entidades emisoras de certificados raíz integrado en el firmware:

- Certificado de CA de Cisco Small Business

- Certificado de CA de CyberTrust
- Certificado de CA de VeriSign
- Certificado de CA de Sipura
- Certificado de CA de Linksys

Antes de empezar

Acceda a la página web de administración del teléfono. Consulte Acceso a la página web del teléfono, en la página 9.

Procedimiento

Paso 1 Seleccione **Información** > **Estado**.

Paso 2 Desplácese hasta **Estado de CA personalizado** y consulte los siguientes campos:

- Estado de aprovisionamiento de CA personalizado: indica el estado de aprovisionamiento.
  - El último aprovisionamiento se realizó correctamente el dd/mm/aaa HH:MM:SS; o
  - El último aprovisionamiento falló el dd/mm/aaa HH:MM:SS
- Información de entidad emisora de certificados personalizada: muestra información sobre la CA personalizada.
  - Installed (Instalada): muestra el "valor de CN", donde el "valor de CN" es el valor del parámetro CN del campo Asunto del primer certificado.
  - Not Installed (No instalada): muestra si no hay instalada ninguna CA personalizada.

Administración de perfiles

En esta sección se muestra la formación de perfiles de configuración en la preparación para su descarga. Para explicar la funcionalidad, se usa TFTP desde un ordenador local como método de resincronización, aunque HTTP o HTTPS también se puede usar.

Compresión de un perfil abierto con Gzip

Un perfil de configuración en formato XML puede alcanzar un tamaño bastante grande si el perfil especifica todos los parámetros de forma individual. Para reducir la carga del servidor de aprovisionamiento, el teléfono admite la compresión del archivo XML, mediante el formato de compresión de deflación que admite la utilidad gzip (RFC 1951).

Nota La compresión debe preceder al cifrado para que el teléfono reconozca un perfil XML comprimido y cifrado.

Para la integración en soluciones de servidor de aprovisionamiento back-end personalizado, se puede usar la biblioteca de compresión zlib código abierto en lugar de la utilidad gzip independiente para realizar la compresión de perfil. Sin embargo, el teléfono espera que el archivo contenga un encabezado gzip válido.

Procedimiento

Paso 1 Instale gzip en el equipo local.

Paso 2 Comprima el perfil de configuración `basic.txt` (se describe en la sección Resincronización TFTP, en la página 53) invocando gzip desde la línea de comandos:

```
gzip basic.txt
```

Esto genera el archivo desinflado `basic.txt.gz` .

Paso 3 Guarde el archivo `basic.txt.gz` en el directorio de raíz virtual del servidor TFTP.

Paso 4 Modificar la regla Profile_Rule en el dispositivo de prueba para resincronizar con el archivo desinflado en lugar del archivo XML original, como se muestra en el ejemplo siguiente:

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

Paso 5 Haga clic en **Submit All Changes** (Enviar todos los cambios).

Paso 6 Tenga en cuenta el seguimiento de Syslog desde el teléfono.

Tras la resincronización, el teléfono descarga el archivo nuevo y lo usa para actualizar sus parámetros.

Temas relacionados

Compresión de perfil abierto, en la página 20

Cifrado de un perfil con OpenSSL

Un perfil comprimido o sin comprimir puede cifrarse (sin embargo, se debe comprimir el archivo antes de su cifrado). El cifrado resulta útil cuando la confidencialidad de la información del perfil es de especial importancia, como cuando se usa TFTP o HTTP para la comunicación entre el teléfono y el servidor de aprovisionamiento.

El teléfono es compatible con el cifrado de claves simétricas mediante el algoritmo AES de 256 bits. Este cifrado puede realizarse mediante el paquete OpenSSL código abierto.

Procedimiento

Paso 1 Instale OpenSSL en un equipo local. Esto puede requerir que se vuelva a compilar la aplicación OpenSSL para activar AES.

Paso 2 Mediante el archivo de configuración `basic.txt` (se describe en la sección Resincronización TFTP, en la página 53), genere un archivo cifrado con el comando siguiente:

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

El archivo comprimido `basic.txt.gz` que se creó en Compresión de un perfil abierto con Gzip, en la página 67 también se puede usar porque el perfil XML se puede comprimir y cifrar.

Paso 3 Guarde el archivo `basic.cfg` cifrado en el directorio raíz virtual del servidor TFTP.

Paso 4 Modifique la regla Profile_Rule del dispositivo de prueba para resincronizar con el archivo cifrado en lugar del archivo XML. La clave de cifrado se comunica al teléfono con la siguiente opción URL:

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

Paso 5 Haga clic en **Submit All Changes** (Enviar todos los cambios).

Paso 6 Tenga en cuenta el seguimiento de Syslog desde el teléfono.

Tras la resincronización, el teléfono descarga el archivo nuevo y lo usa para actualizar sus parámetros.

Temas relacionados

Cifrado AES-256-CBC, en la página 21

Creación de perfiles con particiones

Un teléfono descarga varios perfiles independientes durante cada resincronización. Esta práctica permite la administración de los distintos tipos de información de perfil en distintos servidores y el mantenimiento de los valores de parámetro de configuración comunes que son distintos de los valores específicos de cuenta.

Procedimiento

Paso 1 Cree un nuevo perfil XML `basic2.txt`, que especifique un valor para un parámetro que lo diferencie de los ejercicios anteriores. Por ejemplo, agregue lo siguiente al perfil `basic.txt`:

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

Paso 2 Guarde el perfil `basic2.txt` en el directorio raíz virtual del servidor TFTP.

Paso 3 Deje la primera regla de perfil de los ejercicios anteriores en la carpeta, pero configure la segunda regla del perfil (Profile_Rule_B) para apuntar al nuevo archivo:

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

Paso 4 Haga clic en **Submit All Changes** (Enviar todos los cambios).

El teléfono ahora se resincroniza a los perfiles primero y segundo, en ese orden, siempre que expire una operación de resincronización.

Paso 5 Tenga en cuenta el seguimiento de syslog para confirmar el comportamiento esperado.

Configurar el encabezado de privacidad del teléfono

Un encabezado de privacidad de usuario en el mensaje SIP establece las necesidades de privacidad de usuario de la red de confianza.

Puede establecer el valor del encabezado de privacidad de usuario para cada extensión de línea con una etiqueta XML en el archivo `config.xml`.

Las opciones de encabezado de privacidad son:

- Disabled (predeterminado)
- none: el usuario solicita que un servicio de privacidad no aplique ninguna función de privacidad a este mensaje SIP.
- header: el usuario necesita que un servicio de privacidad oculte los encabezados de los que no se puede purgar información de identificación.
- session: el usuario solicita que un servicio de privacidad proporcione anonimato para las sesiones.
- user: el usuario solicita un nivel de privacidad solo de intermediarios.
- id: el usuario solicita que el sistema utilice un identificador que no muestre el nombre de host o la dirección IP.

Procedimiento

Paso 1 Edite el archivo `config.xml` en un editor de texto o XML.

Paso 2 Inserte la etiqueta **<Privacy_Header_N_ ua="na">*Valor*</Privacy_Header_N_>**, donde N es el número de extensión de línea (1–10) y utilice uno de los siguientes valores.

- Valor predeterminado: **Disabled**
- **ninguno**
- **encabezado**
- **session**
- **user**
- **ID**

Paso 3 (Opcional) Aprovisione las extensiones de línea adicionales usando la misma etiqueta con el número de extensión de línea necesario.

Paso 4 Guarde los cambios en el archivo `config.xml`.

CAPÍTULO 5

Parámetros de aprovisionamiento

Descripción general de los parámetros de aprovisionamiento

En este capítulo se describen los parámetros de aprovisionamiento que se pueden usar en secuencias de comandos de perfil de configuración.

Parámetros de perfil de configuración

La tabla siguiente define la función y el uso de cada parámetro de la sección **Parámetros de perfil de configuración** de la ficha **Aprovisionamiento**.

Nombre de parámetro	Descripción y valor predeterminado
Provision Enable (Activación de aprovisionamiento)	Controla todas las acciones de resincronización, independientemente de las acciones de actualización de firmware. Establezca **Sí** para habilitar el aprovisionamiento remoto. El valor predeterminado es Sí.
Resync On Reset (Resincronizar al restablecer)	Activa una resincronización después de cada reinicio excepto para reinicios provocados por las actualizaciones del firmware y las actualizaciones de parámetros. El valor predeterminado es Sí.

Nombre de parámetro	Descripción y valor predeterminado
Retraso aleatorio de resincronización	Un retraso aleatorio tras la secuencia de arranque antes de realizar el restablecimiento, especificado en segundos. En un grupo de dispositivos de telefonía IP programados para encenderse de forma simultánea, este valor introduce una separación en la hora a la que cada unidad envía una solicitud de resincronización al servidor de aprovisionamiento. Esta función puede resultar útil en una gran implementación residencial, en caso de que se produzcan cortes de energía regionales. El valor de este campo debe ser un número entero entre 0 y 65535. El valor predeterminado es 2.
Resync At (HHmm) [Resincronización a las (HHmm)]	Las horas y minutos (HHmm) en que el dispositivo se resincroniza con el servidor de aprovisionamiento. El valor de este campo debe ser un número de cuatro dígitos entre 0000 y 2400 para indicar la hora en formato HHmm. Por ejemplo, 0959 indica 09:59. El valor predeterminado es vacío. Si el valor no es válido, el parámetro se ignora. Si este parámetro se establece con un valor válido, se omite el parámetro de resincronización periódica.
Resync Random Delay (Retraso aleatorio de resincronización)	Impide una sobrecarga del servidor de aprovisionamiento cuando se enciende un gran número de dispositivos al mismo tiempo. Para evitar una avalancha de solicitudes de resincronización al servidor de varios teléfonos, el teléfono se resincroniza en el intervalo entre las horas y minutos, y las horas y minutos más el retraso aleatorio (hhmm, hhmm + retraso aleatorio). Por ejemplo, si el retraso aleatorio = (resincronización en retraso aleatorio + 30)/60 minutos, el valor de entrada en segundos se convierte a minutos y se redondea al minuto siguiente para calcular el intervalo de retraso aleatorio final. El valor válido está entre 0 y 65535. Esta función está desactivada cuando este parámetro se establece en cero. El valor predeterminado es 600 segundos (10 minutos).

Nombre de parámetro	Descripción y valor predeterminado
Resync Periodic (Resincronización periódica)	Intervalo de tiempo entre resincronizaciones periódicas con el servidor de aprovisionamiento. El temporizador de resincronización asociado está activo solo después de la primera sincronización correcta con el servidor. Los formatos válidos son los siguientes: • Un entero Ejemplo: una entrada de **`3000`** indica que la siguiente resincronización se produce en 3000 segundos. • Varios enteros Ejemplo: una entrada de **`600,1200,300`** indica que la primera resincronización se produce en 600 segundos, la segunda en 1200 segundos después de la primera y la tercera en 300 segundos después de la segunda. • Un intervalo de tiempo Ejemplo: una entrada de **`2400+30`** indica que la siguiente resincronización se produce entre 2400 y 2430 segundos después de una resincronización correcta. Configure este parámetro en cero para deshabilitar la resincronización periódica. El valor predeterminado es 3600 segundos.

Nombre de parámetro	Descripción y valor predeterminado
Resync Error Retry Delay (Retraso de reintento por error de resincronización)	Si una operación de resincronización provoca un error porque el dispositivo de telefonía IP no puede recuperar un perfil del servidor, el archivo descargado está dañado o si se produce un error interno, el dispositivo intenta volver a resincronizarse cuando transcurra el tiempo especificado en segundos. Los formatos válidos son los siguientes: • Un entero Ejemplo: una entrada de **300** indica que el siguiente reintento se produce en 300 segundos. • Varios enteros Ejemplo: una entrada de **600,1200,300** indica que el primer reintento se produce en 600 segundos, el segundo en 1200 segundos después del primero y el tercero en 300 segundos después del segundo. • Un intervalo de tiempo Ejemplo: una entrada de **2400+30** indica que el siguiente reintento se produce entre 2400 y 2430 segundos después de una resincronización con error. Si el retraso se define en 0, el dispositivo no intenta volver a resincronizarse después de un intento fallido.
Forced Resync Delay (Retraso de resincronización forzada)	Retraso máximo (en segundos) que el teléfono debe esperar antes de realizar una resincronización. El dispositivo no se resincroniza mientras se encuentra activa una de sus líneas de teléfono. Como una resincronización puede tardar varios segundos, sería conveniente esperar hasta que el dispositivo haya estado inactivo durante un periodo prolongado para la resincronización. Esto permite al usuario realizar llamadas en sucesión sin interrupciones. El dispositivo tiene un temporizador que inicia la cuenta atrás cuando todas las líneas están inactivas. Este parámetro es el valor inicial del contador. Los eventos de resincronización se retrasan hasta que este contador se reduce a cero. El valor válido está entre 0 y 65535. El valor predeterminado es 14.400 segundos.

Nombre de parámetro	Descripción y valor predeterminado
Resync From SIP (Resincronizar desde SIP)	Permite que se active una resincronización a través de un mensaje NOTIFY de SIP. El valor predeterminado es Sí.
Resincronizar tras intento de actualización	Activa o desactiva la operación de resincronización después de que se produzca cualquier actualización. Si se selecciona Sí, se activa la sincronización. El valor predeterminado es Sí.
Activador de resincronización 1, Activador de resincronización 2	Condiciones de activación de la resincronización configurables. Una resincronización se activa cuando la ecuación lógica de estos parámetros se evalúa como verdadera. El valor predeterminado es (vacío).
Error de resincronización si no se encuentra el archivo	Se considera que una resincronización no se ha realizado correctamente si no se recibe un perfil solicitado del servidor. Eso se puede sustituir por este parámetro. Si el valor definido es **no**, el dispositivo acepta una respuesta `file-not-found` (archivo no encontrado) del servidor como resincronización correcta. El valor predeterminado es Sí.
Regla del perfil Regla del perfil B Regla del perfil C Regla del perfil D	Cada regla de perfil informa al teléfono de un origen del que se obtiene un perfil (archivo de configuración). Durante cada operación de resincronización, el teléfono aplica todos los perfiles en secuencia. Valor predeterminado: **`/$PSN.xml`** Si desea aplicar el cifrado AES-256-CBC a los archivos de configuración, especifique la clave de cifrado con la palabra clave **`--key`** del siguiente modo: **`[--key <clave de cifrado>]`** También puede incluir la clave de cifrado entre comillas (").
Opción de DHCP que se debe usar	Las opciones DHCP, delimitadas por comas, que se usan para recuperar el firmware y los perfiles. El valor predeterminado es 66,160,159,150,60,43,125.

Nombre de parámetro	Descripción y valor predeterminado
Log Request Msg (Mensaje de solicitud de registro)	Este parámetro contiene el mensaje que se envía al servidor syslog al inicio de un intento de resincronización. El valor predeterminado es `$PN $MAC -Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Log Success Msg (Mensaje de registro correcto)	El mensaje de syslog emitido cuando se completa correctamente un intento de resincronización. El valor predeterminado es `$PN $MAC -Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Log Failure Msg (Mensaje de error de registro)	El mensaje de syslog emitido después de un intento de resincronización erróneo. El valor predeterminado es `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync (Resincronización configurable por el usuario)	Permite a un usuario resincronizar el teléfono desde la pantalla del teléfono IP. El valor predeterminado es Sí.

Parámetros de actualización de firmware

La tabla siguiente define la función y el uso de cada parámetro de la sección **Actualización de firmware** de la ficha **Aprovisionamiento**.

Nombre de parámetro	Descripción y valor predeterminado
Upgrade Enable (Activar actualización)	Permite las operaciones de actualización del firmware independientemente de las acciones de resincronización. El valor predeterminado es Sí.
Upgrade Error Retry Delay (Retraso de reintento tras error de actualización)	El intervalo de reintentos de actualización (en segundos) aplicado en caso de una actualización incorrecta. El dispositivo tiene temporizador de error de actualización de firmware que se activa tras un intento de actualización de firmware incorrecto. El temporizador se inicializa con el valor de este parámetro. El próximo intento de actualización del firmware se produce cuando la cuenta atrás de este temporizador llega a cero. El valor predeterminado es 3600 segundos.

Nombre de parámetro	Descripción y valor predeterminado
Regla de actualización	Un script de actualización del firmware que define las condiciones de actualización y las URL del firmware asociadas. Emplea la misma sintaxis que la regla de perfil. Utilice el formato siguiente para introducir la regla de actualización: **<tftp|http|https>://<ip address>/image/<load name>** Por ejemplo: **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Si no se especifica ningún protocolo, se utiliza TFTP. Si no se especifica ningún nombre de servidor, se usa en su lugar el host que solicita la URL. Si no se especifica ningún puerto, se usa el predeterminado (69 para TFTP, 80 para HTTP o 443 para HTTPS). El valor predeterminado es "en blanco".
Mensaje de solicitud de actualización de registro	Mensaje de syslog emitido al inicio de un intento de actualización del firmware. Valor predeterminado: `$PN $MAC--Solicitud de actualización $SCHEME://$SERVIP:$PORT$PATH`
Mensaje de actualización de registro correcta	Mensaje de syslog emitido después de que el intento de actualización del firmware se complete correctamente. El valor predeterminado es `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`
Mensaje de error de actualización de registro	Mensaje de syslog emitido después de un intento de actualización del firmware erróneo. El valor predeterminado es `$PN $MAC -- Upgrade failed: $ERR`
Uso compartido del firmware en el grupo	Activa o desactiva la función Compartir firmware en el grupo. Seleccione **Sí** o **No** para activar o desactivar la función. Valor predeterminado: Sí
Servidor de registro de uso compartido de firmware en el grupo	Indica la dirección IP y el puerto al que se envía el mensaje UDP. Por ejemplo: 10.98.76.123:514 donde, 10.98.76.123 es la dirección IP y 514 es el número de puerto.

Parámetros de uso general

La tabla siguiente define la función y el uso de cada parámetro de la sección **Parámetros de uso general** de la ficha **Aprovisionamiento**.

Nombre de parámetro	Descripción y valor predeterminado
GPP A - GPP P	Los parámetros GPP_* de uso general se emplean como registros de texto libre cuando se configuran los teléfonos para interactuar con una solución de servidor de aprovisionamiento particular. Se pueden configurar para que incluyan varios valores, como estos: • Claves de cifrado • URL • Información de estado de aprovisionamiento multifase • Plantillas de solicitudes posteriores • Asignaciones de alias de nombre de parámetro • Valores de cadena parcial, combinadas al final en valores de parámetros completos El valor predeterminado es "en blanco".

Variables de expansión de macro

Se reconocen determinadas variables macro dentro de los siguientes parámetros de aprovisionamiento:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (en condiciones específicas)

Dentro de estos parámetros, se reconocen y se expanden los tipos de sintaxis, como $NAME o $(NAME).

Se pueden especificar subcadenas de variable macro con la anotación $(NAME:p) y $(NAME:p:q), donde p y q son números enteros no negativos (disponibles en la revisión 2.0.11 y superior). La expansión de macro resultante es la subcadena que empieza en un desplazamiento de carácter p, con la longitud q (o hasta el final de cadena si no se especifica q). Por ejemplo, si GPP_A contiene ABCDEF, a continuación, $(A:2) se expandirá a CDEF y $(A:2:3) se expandirá a CDE.

No se traduce un nombre no reconocido y el formulario $NAME o $(NAME) permanece sin cambios en el valor del parámetro tras la expansión.

Nombre de parámetro	Descripción y valor predeterminado
$	El formulario $$ se expande a un solo carácter $.
A a P	Se sustituye por el contenido de los parámetros generales GPP_A a GPP_P.
SA a SD	Sustituido por los parámetros de propósito especial GPP_SA a GPP_SD. Estos parámetros contienen teclas o contraseñas utilizadas en el aprovisionamiento. **Nota** $SA a $SD se reconocen como argumentos del calificador de direcciones URL de resincronización opcional, --key.
MA	Dirección MAC que usa dígitos hexadecimales en minúsculas, por ejemplo, 000e08aabbcc.
MAU	Dirección MAC que usa dígitos hexadecimales en mayúsculas, por ejemplo, 000E08AABBCC.
MAC	Dirección MAC que usa dígitos hexadecimales en minúsculas y dos puntos para separar los pares de dígitos hexadecimales. Por ejemplo, 00:0e:08:aa:bb:cc.
PN	Nombre de producto. Por ejemplo, CP-6841-3PCC.
PSN	Número de serie del producto. Por ejemplo, 6841-3PCC.
SN	Cadena de número de serie, por ejemplo, 88012BA01234.
CCERT	Estado del certificado de cliente de SSL: Instalado o No instalado.
IP	Dirección IP del teléfono dentro de la subred local. Por ejemplo, 192.168.1.100.
EXTIP	Dirección IP externa del teléfono, tal como se muestra en Internet. Por ejemplo, 66.43.16.52.
SWVER	Cadena de la versión de software. Por ejemplo, sip68xx.11-0-1MPP.
HWVER	Cadena de la versión de hardware. Por ejemplo, 2.0.1

Nombre de parámetro	Descripción y valor predeterminado
PRVST	Estado de aprovisionamiento (una cadena numérica): -1 = solicitud de resincronización explícita 0 = resincronización de encendido 1 = resincronización periódica 2 = error de resincronización, reintento
UPGST	Estado de actualización (una cadena numérica): 1 = primer intento de actualización 2 = error de actualización, reintento
UPGERR	Mensaje del resultado (ERR) de un intento de actualización anterior; por ejemplo, Error de http_get.
PRVTMR	Segundos desde el último intento de resincronización.
UPGTMR	Segundos desde el último intento de actualización.
REGTMR1	Segundos desde que la línea 1 perdió el registro con el servidor SIP.
REGTMR2	Segundos desde que la línea 2 perdió el registro con el servidor SIP.
UPGCOND	Nombre de macro heredada.
SCHEME	Esquema de acceso de archivos, uno de TFTP, HTTP o HTTPS, obtenido después de analizar la dirección URL de resincronización o actualización.
SERV	Solicitud de nombre de host del servidor de destino, según se obtiene después de analizar la URL de resincronización o actualización.
SERVIP	Solicitud de dirección IP del servidor de destino, según se obtiene después de analizar la dirección URL de resincronización o actualización, posiblemente después de la búsqueda de DNS.
PUERTO	Solicitud de puertos UDP/TCP de destino, según se obtienen después de analizar la dirección URL de resincronización o actualización.
PATH	Solicitud de ruta del archivo de destino, según se obtienen después de analizar la dirección URL de resincronización o actualización.

Nombre de parámetro	Descripción y valor predeterminado
ERR	Mensaje del resultado del intento de resincronización o actualización. Solo es útil para generar los mensajes de syslog de resultado. El valor se conserva en la variable UPGERR en el caso de los intentos de actualización.
UIDn	Contenido del parámetro de configuración Line n UserID.
EMS	Estado de Extension Mobility
MUID	ID de usuario de Extension Mobility
MPWD	Contraseña de Extension Mobility

Códigos de error interno

El teléfono define un número de códigos de error interno (X00–X99) para facilitar la configuración del suministro de mayor control sobre el comportamiento de la unidad en determinadas condiciones de error.

Nombre de parámetro	Descripción y valor predeterminado
X00	Error de capa de transporte (o ICMP) al enviar una solicitud SIP.
X20	SIP agota el tiempo de solicitud durante la espera de una respuesta.
X40	Error de protocolo de general SIP (por ejemplo, códec inaceptable en SDP en 200 y mensajes de notificación de aceptación o se agota el tiempo de espera de confirmación).
X60	Número marcado no válido según el plan de marcación especificado.

APÉNDICE A

Ejemplo de perfiles de configuración

Ejemplo de formato abierto 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>
```

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

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

Ejemplo de perfiles de configuración

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

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

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

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

Ejemplo de perfiles de configuración

APÉNDICE B

Acrónimos

Acrónimos

AC	Corriente alterna
ACS	Servidor de control de acceso
A/D	Convertidor de analógico a digital
AES	estándar de cifrado avanzado
ANC	Llamada anónima
AP	Punto de acceso
ASCII	Código Estándar Americano para el Intercambio de Información
B2BUA	Agente de usuario Back to Back
BLF	luz de ocupado
Bool	Valores booleanos. Se especifican como sí y no, o 1 y 0 en el perfil
BootP	Protocolo bootstrap
CA	Entidad emisora de certificados
CAS	Señal de alerta CPE
CDP	Cisco Discovery Protocol
CDR	Registro de detalle de llamadas
CGI	Imágenes generadas por ordenador
CID	Identificar a la persona que llama
CIDCW	ID del autor de la llamada de espera de llamada

CNG	Generación de ruido de fondo confortable
CPC	Control de autor de la llamada
CPE	Equipamiento de las instalaciones del cliente
CSV	Valor separado por comas
CWCID	ID del autor de la llamada de espera de llamada
CWT	Tono de espera de llamada
D/A	Convertidor de digital a analógico
dB	Decibelios
dBm	dB con respecto a 1 milivatio
DHCP	Protocolo de configuración dinámica del host
NoMlsta	No molestar
DNS	Sistema de nombre de dominio
DoS	Denegación de servicio
DRAM	Memoria de acceso aleatorio dinámico
DSL	Bucle de suscriptor digital
DSP	Procesador de señal digital
DST	Horario de verano
DTAS	Señal de alerta de terminal de datos (igual que CAS)
DTMF	Tonos duales de multifrecuencia
FQDN	Nombre de dominio completamente calificado
FSK	Afinamiento del cambio de frecuencia
FW	Firmware
FXS	Foreign eXchange Station
GMT	Hora media de Greenwich
GW	Gateway (Puerta de enlace)
HTML	Lenguaje de marcado de hipertexto
HTTP	Protocolo de transferencia de hipertexto
HTTPS	HTTP sobre SSL
ICMP.	Protocolo de mensajes de control de Internet

FUNCIONES DE ENVÍO	Protocolo de administración de grupos de Internet
ILEC	Proveedor de telecomunicaciones locales dominante
IP	Protocolo de Internet
IPv4	Protocolo de Internet versión 4
IPv6	Protocolo de Internet versión 6
ISP	Proveedor de servicios de Internet
ITSP	Proveedor de servicios de telefonía de Internet
ITU	Unión internacional de telecomunicaciones (International Telecommunication Union)
IVR	Respuesta interactiva de voz
LAN	Red de área local
LBR	Velocidad de bits baja
LBRC	Códec de velocidad de bits baja
LCD	Pantalla de cristal líquido; también conocido como pantalla
LDAP	LDAP (protocolo ligero de acceso a directorios)
LED	Diodo emisor de luz
Dirección MAC	Dirección de control de acceso a los medios
MC	Certificado mínima
MGCP	Protocolo de control de gateway de medios.
MOH	Música en espera
MOS	Puntuación de opinión media (1-5, cuanto mayor sea, mejor)
MPP	Teléfonos multiplataforma
ms	Milisegundo
MSA	Adaptador de origen de música
MWI	Indicación de mensaje en espera
NAT	Traducción de direcciones de red
NPS	Servidor de aprovisionamiento normal
NTP	Protocolo de tiempo de red
OOB	Fuera de banda

OSI	Intervalo de comunicación abierto
PBX (del inglés Private Branch Exchange)	Centralita privada
PCB	Placa de circuito impreso
PoE	Power over Ethernet
PR	Inversión de polaridad
PS	Servidor de aprovisionamiento
PSQM	Medición de calidad perceptual de voz (1-5, cuanto menor, mejor)
PSTN	Red telefónica pública conmutada
QoS	Calidad de servicio (QoS)
CR	Eliminar la personalización
REQT	(SIP) Mensaje de solicitud
RESP	(SIP) Mensaje de respuesta
RSC	(SIP) Código de estado de respuesta, por ejemplo, 404, 302, 600
RTP	Protocolo en tiempo real
RTT	Tiempo de ida y vuelta
SAS	Servidor de transmisión de Audio
SDP	Protocolo de descripción de sesión
SDRAM	DRAM sincrónica
s	segundos
SIP	Protocolo de inicio de sesión (Session Initiation Protocol)
SLA	Apariencia de línea compartida
SLIC	Circuito de interfaz de línea del suscriptor
SP	Proveedor de servicios
SSL	Capa de socket seguro
STUN	UDP transversal de sesión para NAT
TCP	Protocolo de control de transmisión
TFTP	Protocolo de transferencia de archivos trivial

TLS	Seguridad de la capa de transporte
TTL	Tiempo de vida
ToS	Tipo de servicio
UA	Agente de usuario
uC	Controlador de Micro
UDP	Protocolo de datagramas de usuario
URI	Identificador uniforme de recursos
URL	Localizador uniforme de recursos
UTC	Hora universal coordinada
VAR	Revendedor de valor añadido
VLAN	LAN de voz
VM	Buzón de voz
VMWI	Indicación/Indicador visual de mensaje en espera
VoIP	Protocolo de voz sobre Internet
VQ	Calidad de voz
WAN	Red de área amplia
XML	Lenguaje de marcado extensible

Acrónimos

APÉNDICE C

Documentación relacionada

Documentación relacionada

Use las secciones siguientes para obtener información relacionada.

Documentación del Cisco IP Phone serie 6800

Consulte las publicaciones específicas para su idioma, modelo de teléfono y versión de firmware multiplataforma. Desplácese desde el Localizador uniforme de recursos (URL) siguiente:

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

Política de compatibilidad del firmware de Cisco IP Phone

Para obtener información sobre la política de asistencia de los teléfonos, consulte https://cisco.com/go/phonefirmwaresupport.