Guide de mise à disposition des téléphones multiplateformes IP Cisco 6800

Première publication: 22 Novembre 2017

Dernière modification: 5 Août 2019

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)

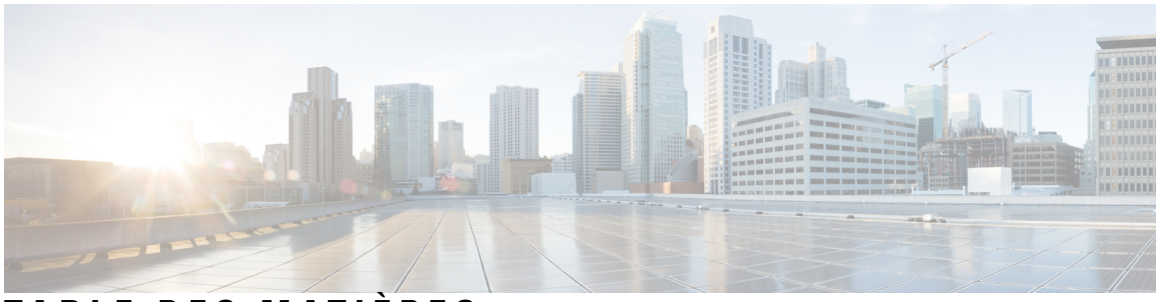
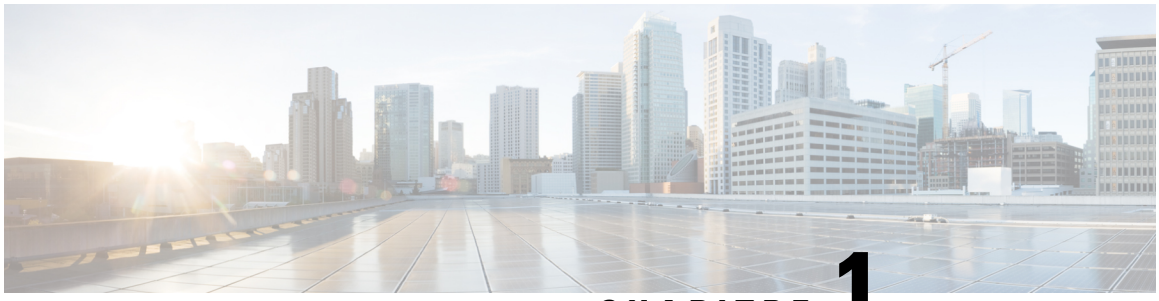


TABLE DES MATIÈRES



CHAPITRE 1

Déploiement et mise à disposition

Nouveautés et mises à jour

Nouveautés et modifications de la version 11.2(4) du micrologiciel

Révision	Nouvelles sections ou sections modifiées
Ajout de paramètres pour les paramètres Wi-Fi	Exemple de Format Open XML, à la page 83

Nouveautés et modifications de la version 11.2(3) SR1 du micrologiciel

Les sections suivantes sont nouvelles ou mises à jour pour prendre en charge les Téléphones multiplateformes IP Cisco 6800.

Révisions	Nouvelles sections ou sections modifiées
Ajout d'une nouvelle rubrique permettant l'intégration par code d'activation.	Intégrer votre téléphone avec le code d'activation , à la page 11

Nouveautés et modifications de la version 11.2(3) du micrologiciel

Les sections suivantes sont nouvelles ou mises à jour pour prendre en charge les Téléphones multiplateformes IP Cisco 6800.

Révisions	Nouvelles sections ou sections modifiées
Ajout d'une rubrique de concept pour le chiffrement de profil ouvert.	Chiffrement de profil ouvert, à la page 20
Ajout d'une nouvelle rubrique pour introduire le chiffrement du contenu HTTP en fonction de RFC 8188.	Chiffrement du contenu HTTP en fonction de RFC-8188, à la page 24
Mise à jour avec des informations détaillées sur le cryptage RFC 8188.	Formats de profil de configuration, à la page 15 Mise à disposition HTTP, à la page 45
Mise à jour des informations détaillées de l'introduction pour le chiffrement de profil ouvert.	Chiffrement AES-256-CBC, à la page 21
Mise à jour de la description de l'option `-key` et ajout d'une remarque sur le cryptage RFC 8188.	key, à la page 25 Paramètres de profil de configuration, à la page 71
Mise à jour des exemples de format open XML avec de nouveaux paramètres et options disponibles	Exemple de Format Open XML, à la page 83

Nouveautés et modifications de la version 11.2(1) du micrologiciel

Révisions	Nouvelles sections ou sections modifiées
Mise à jour de la rubrique avec une référence à la comparaison des paramètres XML et TR69	Mise à disposition TR69, à la page 4
Ajout d'une nouvelle rubrique pour prendre en charge la fonction d'en-tête de confidentialité	Définir l'en-tête de confidentialité du téléphone, à la page 68
Ajout d'une nouvelle rubrique pour prendre en charge le partage de micrologiciel par les homologues	Partage de micrologiciel par les homologues, à la page 12
Mise à jour de cette rubrique avec les méthodes de chiffrement	Obtenir un certificat de serveur signé, à la page 48
Mise à jour de cette rubrique pour prendre en charge la fonctionnalité d'évitement de l'écran **Définir le mot de passe**	Configuration du contrôle d'accès, à la page 9
Ajout d'une nouvelle rubrique pour prendre en charge l'évitement de l'écran **Définir le mot de passe**	Ignorer l'écran Définir le mot de passe, à la page 13

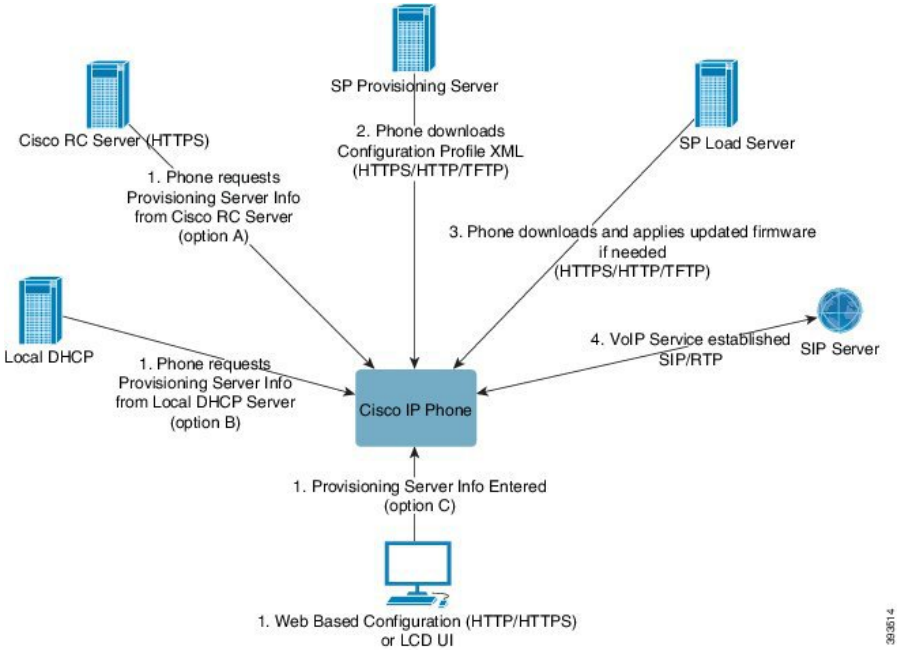
Présentation de la mise à disposition

Les téléphones IP Cisco sont destinés aux déploiements volumineux effectués par des fournisseurs de service de voix sur IP (VoIP) aux clients dans des environnements résidentiels, de petite ou grande entreprise. Par conséquent, mettre à disposition le téléphone en utilisant la configuration et la gestion à distance permet d'assurer le bon fonctionnement du téléphone sur le site du client.

Cisco prend en charge la configuration personnalisée et continue des fonctions du téléphone en utilisant les fonctions :

- Contrôle à distance fiable du téléphone.
- Chiffrement de la communication qui contrôle le téléphone.
- Liaison du compte téléphonique simplifiée.

Les téléphones peuvent être mis à disposition pour télécharger les profils de configuration ou les mises à jour du micrologiciel à partir d'un serveur distant. Les téléchargements peuvent se produire lorsque les téléphones sont connectés à un réseau, lorsqu'ils sont mis sous tension et à intervalles réguliers. La mise à disposition est généralement effectuée dans le cadre de déploiements VoIP de grande envergure, courants chez les fournisseurs de service. Les profils de configuration et/ou les micrologiciels mis à jour sont transférés sur le périphérique par TFTP, HTTP ou HTTPS.



En synthèse, le processus de mise à disposition du téléphone est le suivant :

1. Si le téléphone n'est pas configuré, les informations de mise à disposition du serveur sont appliquées au téléphone en utilisant l'une des options suivantes :
   - **A** : téléchargées à partir du serveur de personnalisation à distance (RC) du Cisco Enablement Data Orchestration System (EDOS) en utilisant HTTPS.
   - **B** : obtenues à partir d'un serveur DHCP local.

- **C** : saisies manuellement via l'utilitaire de configuration web du téléphone Cisco ou son interface utilisateur.

2. Le téléphone télécharge les informations du serveur de mise à disposition et applique le XML de configuration en utilisant le protocole HTTPS, HTTP ou TFTP.
3. Le téléphone télécharge et applique les micrologiciels mis à jour, si nécessaire, en utilisant HTTPS, HTTP ou TFTP.
4. Le service VoIP est établi en utilisant la configuration et le micrologiciel spécifiés.

Les fournisseurs de services VoIP ont l'intention de déployer de nombreux téléphones chez les clients résidentiels et les petites entreprises. Dans les environnements de petites et grandes entreprises, les téléphones peuvent servir de nœuds de terminal. Les fournisseurs distribuent largement ces appareils sur Internet, qui sont connectés par l'intermédiaire de routeurs et de pare-feu dans les locaux du client.

Le téléphone peut être utilisé comme une extension à distance de l'équipement back-end du fournisseur de services. La configuration et la gestion à distance assurent le bon fonctionnement du téléphone dans les locaux du client.

Mise à disposition TR69

Le téléphone IP Cisco aide l'administrateur à configurer les paramètres du TR69 à l'aide de l'interface utilisateur Web. Pour des informations relatives aux paramètres, y compris une comparaison des paramètres XML et TR69, reportez-vous au Guide d'Administration de la série de téléphone correspondante.

Les téléphones prennent en charge la détection automatique du serveur de configuration (ACS) à partir de l'Option DHCP 43, 60 et 125.

- Option 43 : informations spécifiques au fournisseur pour l'URL ACS.
- Option 60 : identifiant de classe du fournisseur afin que le téléphone s'identifie lui-même avec `dslforum.org` auprès de l'ACS.
- Option 125 : informations spécifiques au fournisseur pour l'association de la passerelle.

Méthodes RPC

Méthodes RPC prises en charge

Les téléphones ne prennent en charge qu'un nombre limité de méthodes RPC (D'appel de procédure à distance) :

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames

- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download : téléchargez la méthode RPC, les types de fichier pris en charge sont :
  - Image de mise à niveau du micrologiciel
  - Fichier de configuration du fournisseur
  - Fichier d'autorité de certification (CA, Certificate Authority) personnalisé
- Transfer Complete

Types d'événements pris en charge

Les téléphones prennent en charge les types d'événements basés sur les fonctions et les méthodes prises en charge. Seuls les types d'événements suivants sont pris en charge :

- Bootstrap
- Boot
- Value change
- Connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

Chiffrement des communications

Les paramètres de configuration qui sont transmis au périphérique peuvent contenir des codes d'autorisation ou d'autres informations qui protègent le système de tout accès non autorisé. Il est dans l'intérêt du fournisseur de services d'empêcher d'activité non autorisée du client. Il est dans l'intérêt du client d'empêcher l'utilisation non autorisée du compte. Le fournisseur de services peut chiffrer la communication du profil de configuration entre le serveur de mise à disposition et le périphérique, en complément de la possibilité de restreindre l'accès au serveur web d'administration.

Comportement du téléphone pendant les périodes de congestion du réseau

Tout élément susceptible de dégrader la performance du réseau risque d'affecter la qualité vocale du téléphone, et dans certains cas, d'entraîner l'abandon d'un appel. Parmi les sources de dégradation du réseau figurent, de manière non exhaustive, les activités suivantes :

- Les tâches administratives telles qu'une analyse de port interne ou une analyse de sécurité
- Les attaques se produisant sur le réseau, telles que les attaques de déni de service

Déploiement

Les téléphones IP Cisco fournissent des mécanismes pratiques pour le déploiement, en fonction de ces modèles de déploiement :

- Distribution en masse : le fournisseur de service acquiert des téléphones IP Cisco en masse et soit les pré-provisionne en interne ou achète des unités de personnalisation à distance (RC) de Cisco. Les périphériques sont ensuite envoyés aux clients dans le cadre d'un contrat de service VoIP.
- Distribution au détail : le client achète le téléphone IP Cisco dans le commerce et demande des services VoIP au fournisseur de services. Le fournisseur de services doit prendre alors en charge la configuration à distance sécurisée du périphérique.

Distribution en masse

Dans ce modèle, le fournisseur de services distribue les téléphones à ses clients dans le cadre d'un contrat de service VoIP. Les périphériques sont soit des unités RC, soit sont préprovisionnés en interne.

Cisco préprovisionne des unités RC pour les resynchroniser avec un serveur Cisco qui télécharge les mises à jour du micrologiciel et du profil de périphérique.

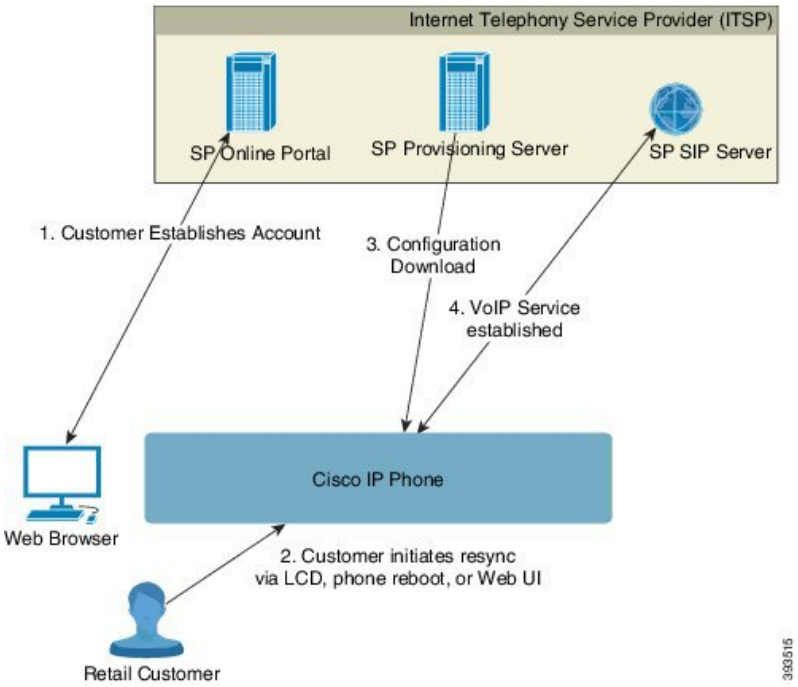
Un fournisseur de services peut préprovisionner les téléphones avec les paramètres souhaités, y compris les paramètres qui contrôlent la resynchronisation, de plusieurs manières :

- En interne à l'aide de DHCP et TFTP
- À distance en utilisant TFTP, HTTP ou HTTPS
- Par une combinaison de mise à disposition en interne et à distance

Distribution de vente au détail

Dans un modèle de distribution de détail, un client achète un téléphone et s'abonne à un service spécifique. Le fournisseur de services de téléphonie Internet (ITSP) configure et gère un serveur de mise à disposition et préprovisionne le téléphone pour le resynchroniser avec le serveur du fournisseur de services.

Illustration 1 : Distribution de vente au détail



Le téléphone inclut l'utilitaire de configuration Web qui affiche la configuration interne et accepte de nouvelles valeurs de paramètres de configuration. Le serveur accepte également une syntaxe de commandes URL spéciale qui permet d'effectuer des opérations de mise à niveau du micrologiciel et de resynchronisation de profil à distance.

Le client se connecte au service et établit un compte VoIP, au moyen d'un portail d'aide en ligne et lie le périphérique au compte de service qui lui a été affecté. Pour ce faire, le téléphone non mis à disposition reçoit l'ordre de se resynchroniser avec un serveur de mise à disposition spécifique via une commande URL de resynchronisation. Généralement, la commande URL inclut un numéro d'ID du client ou un code alphanumérique qui permet d'associer le périphérique au nouveau compte.

Dans l'exemple ci-dessous, un périphérique à l'adresse IP attribuée par le serveur DHCP 192.168.1.102 reçoit l'ordre de se mettre à disposition du service SuperVoIP :

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

Dans cet exemple, 1234abcd est le numéro d'ID du client du nouveau compte. Le serveur de mise à disposition distant associe au nouveau compte le téléphone qui effectue la demande de resynchronisation, en fonction de l'adresse URL et de l'ID du client fourni. Au moyen de cette opération de resynchronisation initiale, le téléphone est configuré en une seule étape. Le téléphone est automatiquement dirigé pour resynchronisation par la suite vers une URL permanente sur le serveur. Par exemple :

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

Pour un accès initial et permanent, le serveur de mise à disposition s'appuie sur le certificat client du téléphone pour l'authentification. Le serveur de mise à disposition fournit des valeurs de paramètre de configuration correctes basées sur le compte de service associé.

Lorsque l'appareil est sous tension ou que le temps spécifié est écoulé, le téléphone se resynchronise et télécharge les derniers paramètres de configuration. Ces paramètres peuvent répondre à des objectifs tels que le paramétrage d'un groupe de recherche, de numéros à numérotation rapide et la limitation des fonctionnalités qu'un utilisateur peut modifier.

Rubriques connexes

Préprovisionnement de périphérique interne, à la page 43

Processus de resynchronisation

Le micrologiciel de chaque téléphone inclut un serveur web d'administration qui accepte les nouvelles valeurs de paramètre de configuration. Le téléphone peut être invité à resynchroniser sa configuration après le redémarrage, ou à intervalles réguliers auprès d'un serveur de mise à disposition spécifié via une commande URL de resynchronisation dans le profil de périphérique.

Par défaut, le serveur web est activé. Pour active ou désactiver le serveur web, utilisez la commande URL de resynchronisation.

Si nécessaire, une resynchronisation immédiate peut-être être demandée via une URL d'action de « resynchronisation ». La commande URL de resynchronisation peut inclure un numéro d'ID de client de compte ou un code alphanumérique qui permet d'associer de manière unique le périphérique au compte utilisateur.

Exemple

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

Dans cet exemple, un périphérique à l'adresse IP attribuée par le serveur DHCP 192.168.1.102 reçoit l'ordre de se mettre à disposition du service SuperVoIP à l'adresse prov.supervoip.com. Le numéro d'ID de client du nouveau compte est 1234abcd. Le serveur de mise à disposition distant associe au compte le téléphone qui effectue la demande de resynchronisation, en fonction de l'adresse URL et de l'ID du client.

Au moyen de cette opération de resynchronisation initiale, le téléphone est configuré en une seule étape. Le téléphone est automatiquement dirigé pour resynchronisation par la suite vers une URL permanente sur le serveur.

Pour un accès initial et permanent, le serveur de mise à disposition s'appuie sur le certificat client pour l'authentification. Le serveur fournit des valeurs de paramètre de configuration basées sur le compte de service associé.

Mise à disposition

Un téléphone peut être configuré afin de resynchroniser son état de configuration interne pour correspondre à un profil à distance, soit périodiquement, soit à la mise sous tension. Le téléphone contacte un serveur de mise à disposition normale (NPS) ou un serveur de contrôle d'accès (ACS).

Par défaut, une resynchronisation de profil n'est tentée que lorsque le téléphone est inactif. Cette pratique empêche une mise à niveau qui déclencherait un redémarrage du logiciel et interromprait l'appel. Si des mises à niveau intermédiaires sont nécessaires pour atteindre un état en cours de mise à niveau depuis une version antérieure, la logique de mise à niveau peut automatiser les mises à niveau à plusieurs étages.

Serveur de mise à disposition normale

Le serveur de mise à disposition normale (NPS) peut être un serveur TFTP, HTTP ou HTTPS. Une mise à niveau du micrologiciel à distance s'effectue via TFTP ou HTTP, ou encore HTTPS, car le micrologiciel ne contient pas d'informations sensibles.

Bien que l'utilisation des HTTPS soit recommandée, la communication avec le serveur de mise à disposition normale ne nécessite pas l'utilisation d'un protocole sécurisé car le profil mis à jour peut-être chiffré par une clé secrète partagée. Pour plus d'informations sur l'utilisation de HTTPS, consultez Chiffrement des communications, à la page 5. La mise à disposition initiale sécurisée est fournie au moyen d'un mécanisme qui utilise la fonctionnalité SSL. Un téléphone non mis à disposition peut recevoir un profil chiffré par une clé symétrique 256 bits destiné à ce périphérique.

Configuration du contrôle d'accès

Le micrologiciel du téléphone fournit des mécanismes pour restreindre l'accès de l'utilisateur final à certains paramètres. Le micrologiciel fournit des privilèges spécifiques pour la connexion à un compte **d'administration** ou à un compte **utilisateur**. Chacun peut être protégé de manière indépendante par un mot de passe.

- Compte d'administrateur : permet l'accès complet du fournisseur de services à tous les paramètres du serveur web d'administration.
- Compte d'utilisateur : permet à l'utilisateur de configurer un sous-ensemble des paramètres du serveur web d'administration.

Le fournisseur de services peut restreindre le compte utilisateur dans le profil de mise à disposition de la manière suivante :

- Indiquer les paramètres de configuration qui sont disponibles pour le compte d'utilisateur lors de la création de la configuration.
- Désactiver l'accès utilisateur au serveur web d'administration.
- Désactiver l'accès utilisateur pour l'interface utilisateur de l'écran LCD.
- Ignorer l'écran **Définir le mot de passe** de l'utilisateur.
- Limiter les domaines Internet accessibles par le périphérique pour la resynchronisation, les mises à niveau ou l'enregistrement SIP pour la ligne 1.

Rubriques connexes

Propriétés de la balise élément, à la page 16
Contrôle d'accès, à la page 18

Accéder à la page web du téléphone

Si votre fournisseur de services a désactivé l'accès à l'utilitaire de configuration, contactez-le avant de continuer.

Procédure

Étape 1 Assurez-vous que l'ordinateur peut communiquer avec le téléphone. Qu'aucun réseau privé virtuel (VPN) n'est en cours d'utilisation.

Étape 2 Ouvrez un navigateur Web.

Étape 3 Saisissez l'adresse IP du téléphone dans la barre d'adresse du navigateur web.

- Accès utilisateur : **`http://<adresse ip>`**
- Accès administrateur : **`http://<adresse ip>/admin/advanced`**
- Accès administrateur : **`http://<adresse ip>`**, cliquez sur **Connexion d'administration** et sur **Avancé**

Par exemple, `http://10.64.84.147/admin/`

Étape 4 Saisissez le mot de passe lorsque vous y êtes invité.

Activation de l'accès Internet au téléphone IP Cisco

Pour afficher les paramètres du téléphone, activez le profil de configuration. Pour modifier n'importe lequel des paramètres, vous devez pouvoir changer le profil de configuration. Votre administrateur système a peut-être désactivé l'option du téléphone qui permet d'afficher l'interface utilisateur web du téléphone ou d'écrire dans cette dernière.

Pour plus d'informations, consultez le *Guide de mise à disposition des téléphones multiplateformes IP Cisco 6800*.

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Cliquez sur **Voix** > **Système**.

Étape 2 Dans la section **Configuration système**, définissez **Enable Web Server** sur **Oui**.

Étape 3 Pour mettre à jour le profil de configuration, cliquez sur **Envoyer toutes les modifications** après avoir modifié les champs de l'interface utilisateur web du téléphone.

Le téléphone redémarre et les modifications sont appliquées.

Étape 4 Pour effacer toutes les modifications effectuées pendant la session en cours (ou après la dernière sélection de **Envoyer toutes les modifications**), cliquez sur **Annuler toutes les modifications**. Les valeurs reviennent à leur paramétrage précédent.

Pratiques de mise à disposition des téléphones

En général, le téléphone IP Cisco est configuré pour la mise à disposition lors de la première connexion au réseau. Le téléphone est également mis à disposition à des intervalles réguliers définis lorsque le VAR (Value Added Retailer, revendeur à valeur ajoutée) préprovisionne (c'est-a-dire configure) le téléphone. Les fournisseurs de services peuvent autoriser les revendeurs à valeur ajoutée ou les utilisateurs avancés à configurer manuellement le téléphone à l'aide de son clavier. Vous pouvez également configurer la mise à disposition à l'aide de l'interface utilisateur web de téléphone.

Vérifiez **l'État** > **État du téléphone** > **Mise à disposition** à partir de l'interface utilisateur LCD du téléphone LCD ou l'état de la mise à disposition sur l'onglet **État** de l'utilitaire de configuration web.

Rubriques connexes

Mettre à disposition manuellement un téléphone à l'aide du clavier, à la page 12

Intégrer votre téléphone avec le code d'activation

Cette fonctionnalité est disponible dans le micrologiciel version 11-2-3MSR1, BroadWorks Application Server version 22.0 (patch AP.as. 22.0.1123. ap368163 et ses dépendances). Toutefois, vous pouvez modifier les téléphones comportant un micrologiciel plus ancien pour pouvoir utiliser cette fonction. Vous indiquez au téléphone qu'il doit effectuer la mise à niveau vers le nouveau micrologiciel et utiliser la règle de profil `gds://` pour déclencher l'écran du code d'activation. Un utilisateur saisit un code à 16 chiffres dans le champ fourni pour intégrer automatiquement le téléphone.

Remarque Le Téléphones multiplateformes IP Cisco 6861 ne prend pas en charge le code d'activation intégré.

Avant de commencer

Assurez-vous que vous autorisez le service d'activation.webex.com par l'intermédiaire de votre pare-feu à prendre en charge l'intégration via le code d'activation.

Procédure

Étape 1 Modifiez le fichier config.xml du téléphone à l'aide d'un éditeur XML ou d'un éditeur de texte.

Étape 2 Suivez l'exemple ci-dessous dans votre fichier config. xml pour définir la règle de profil pour l'intégration par code d'activation.

```
<?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>
```

Étape 3 Enregistrez les modifications apportées au fichier config.xml.

Mettre à disposition manuellement un téléphone à l'aide du clavier

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Administration du périphérique** > **Règle de profil**.

Étape 3 Saisissez la règle de profil en utilisant le format ci-dessous :

```
protocole://serveur[:port]/nom_chemin_profil
```

Par exemple :

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

Lorsqu'aucun protocole n'est spécifié, le protocole par défaut est TFTP. Si aucun nom de serveur n'est spécifié, l'hôte sollicitant l'URL est utilisé en tant que nom de serveur. Lorsqu'aucun port n'est spécifié, le port par défaut est utilisé (69 pour TFTP, 80 pour HTTP ou 443 pour HTTPS).

Étape 4 Appuyez sur **Resync**.

Rubriques connexes

Pratiques de mise à disposition des téléphones, à la page 10

Partage de micrologiciel par les homologues

Le partage de micrologiciels par les homologues (PFS, Peer Firmware Sharing) est un modèle de distribution de micrologiciels qui permet à un téléphone IP Cisco de trouver d'autres téléphones du même modèle ou de la même série sur le sous-réseau et de partager des fichiers de micrologiciel mis à jour lorsque vous devez mettre à niveau plusieurs téléphones simultanément. PFS utilise le protocole Cisco Peer-to-Peer-Distribution Protocol (CPPDP) qui est un protocole propriétaire Cisco. Avec CPPDP, tous les périphériques du sous-réseau forment une hiérarchie homologue à homologue, puis copient le micrologiciel ou les autres fichiers des périphériques homologues vers les périphériques voisins. Pour optimiser les mises à niveau du micrologiciel, un téléphone racine télécharge l'image du micrologiciel à partir du serveur de charge, puis transfère le micrologiciel vers d'autres téléphones du sous-réseau à l'aide de connexions TCP.

Le partage de micrologiciel par les homologues :

- Limite la congestion des transferts TFTP vers des serveurs de charge centralisés distants.
- Élimine la nécessité de contrôler manuellement les mises à niveau de micrologiciel.
- Réduit les temps d'arrêt du téléphone pendant les mises à niveau lorsqu’un grand nombre de téléphones sont simultanément réinitialisés.

Remarque

- Le partage du micrologiciel par les homologues ne fonctionne pas, sauf si plusieurs téléphones sont définis pour la mise à niveau en même temps. Lorsqu'une commande NOTIFY est envoyée avec Event:resync, elle initie une resynchronisation sur le téléphone. Exemple xml qui peut contenir les configurations pour lancer la mise à niveau :

  "Event:resync;profile="http://10.77.10.141/profile.xml
- Lorsque vous définissez le serveur de journal de partage de micrologiciel avec les homologues sur une adresse IP et un port, les journaux spécifiques PFS sont envoyés à ce serveur en tant que messages UDP. Ce paramétrage doit être effectué sur chaque téléphone. Vous pouvez ensuite utiliser les messages du journal lors de la résolution des problèmes liés à PFS.

Peer_Firmware_Sharing_Log_Server spécifie le nom d'hôte et le port du serveur syslog UDP distant. Par défaut, le port est syslog 514.

Par exemple :

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

Pour utiliser cette fonction, activez PFS sur les téléphones.

Ignorer l'écran Définir le mot de passe

Vous pouvez ignorer l'écran **Définir le mot de passe** du téléphone au premier démarrage ou après une réinitialisation d'usine, en fonction de ces actions de mise à disposition :

- Configuration DHCP
- Configuration EDOS
- Configuration du mot de passe de l'utilisateur à l'aide de fichier de configuration XML du téléphone.

Tableau 1 : Actions de mise à disposition qui déterminent si l'écran Définir le mot de passe s'affiche

DHCP configuré	EDOS configuré	Mot de passe utilisateur configuré	Ignorer l'écran Définir le mot de passe
Oui	N/A	Oui	Oui
Oui	N/A	Non	**Non**
Non	Oui	Oui	Oui
Non	Oui	Non	**Non**
Non	Non	N/A	**Non**

Procédure

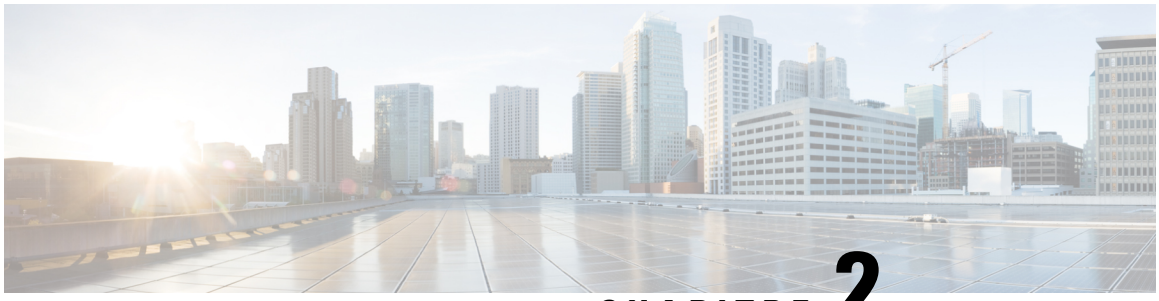
Étape 1 Modifiez le fichier `cfg.xml` du téléphone à l'aide d'un éditeur XML ou d'un éditeur de texte.

Étape 2 Insérez la balise **< User_Password >** en utilisant l'une des options suivantes.

- **Aucun mot de passe (balise de début et de fin)**–**<User_Password></User_Password >**
- **La valeur de mot de passe (entre 4 et 127 caractères)**–**<User_Password ua = "rw" > abc123</User_Password>**
- **Aucun mot de passe (balise de début uniquement)**–**<User_Password/>**

Étape 3 Enregistrez les modifications apportées au fichier `cfg.xml`.

L' écran **Définir le mot de passe** ne s'affiche pas au premier démarrage ou après une réinitialisation d'usine. Si un mot de passe est spécifié, l'utilisateur est invité à saisir le mot de passe lors de l'accès à la page Web du téléphone ou aux menus de l'écran du téléphone.



CHAPITRE 2

Formats de mise à disposition

Scripts de mise à disposition

Le téléphone accepte la configuration au format XML.

Pour des informations détaillées sur votre téléphone, reportez-vous au guide d'administration de votre appareil spécifique. Chaque guide décrit les paramètres pouvant être configurés par le serveur web d'administration.

Formats de profil de configuration

Le profil de configuration définit les valeurs des paramètres du téléphone.

Le format XML de profil de configuration utilise les outils de création standard XML pour compiler les paramètres et les valeurs.

Remarque Seul le jeu de caractères UTF-8 est pris en charge. Si vous modifiez le profil dans un éditeur, ne modifiez pas le format de codage ; dans le cas contraire, le téléphone ne reconnaît pas le fichier.

Chaque téléphone comporte un ensemble de fonctionnalités différentes et, par conséquent, un jeu différent de paramètres.

Profil de Format XML (XML)

Le profil de format ouvert est un fichier texte avec une syntaxe similaire à XML dans une hiérarchie d'éléments, avec des valeurs et des attributs d'élément. Ce format vous permet d'utiliser les outils standard pour créer le fichier de configuration. Un fichier de configuration dans ce format peut être envoyé à partir du serveur de

mise à disposition au téléphone lors de l'opération de resynchronisation. Le fichier peut être envoyé sans compilation comme objet binaire.

Le téléphone peut accepter les formats de configuration que génèrent des outils standard. Cette fonctionnalité facilite le développement d'un logiciel de serveur de mise à disposition de back-end qui génère des profils de configuration à partir de bases de données existantes.

Pour assurer la protection des informations confidentielles du profil de configuration, le serveur de mise à disposition envoie ce type de fichier au téléphone via un canal sécurisé par TLS. Éventuellement, le fichier peut être compressé à l'aide de l'algorithme de compression gzip (RFC1951).

Le fichier peut être chiffré à l'aide de l'une de ces méthodes de chiffrement :

- Chiffrement AES-256-CBC
- Chiffrement du contenu HTTP en fonction de RFC-8188 avec un chiffrement AES-128-GCM

Exemple : profil de format ouvert

```
<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 balise < flat-profile > de l'élément entoure tous les éléments paramètres que le téléphone reconnaît.

Rubriques connexes

Chiffrement et compression de profil ouvert (XML), à la page 20

Composants du fichier de configuration

Un fichier de configuration peut comporter les composants suivants :

- Balises d'élément
- Attributs
- Paramètres
- Fonctions de mise en forme
- Commentaires XML

Propriétés de la balise élément

- Le format XML de mise à disposition et l'interface utilisateur Web permettent la configuration des mêmes paramètres. Le nom de la balise XML et les noms de champ dans l'interface utilisateur Web sont similaires, mais varient en raison des restrictions de nom d'élément XML. Par exemple, des traits de soulignement (_) au lieu de « ».
- Le téléphone reconnaît les éléments comportant des noms de paramètre corrects qui sont encapsulés dans l'élément spécial <flat-profile>.

- Les noms d'élément sont compris entre crochets.
- La plupart des noms d'éléments sont similaires aux noms de champ des pages web d'administration du périphérique, avec les modifications suivantes :
  - Les noms d'éléments ne peuvent pas comporter d'espaces ou de caractères spéciaux. Pour obtenir le nom de l'élément à partir du nom de champ d'administration web, remplacez chaque espace par un trait de soulignement ou les caractères spéciaux `[`, `]`, `(`, `)`, ou `/`.

    Par exemple : l'élément < Resync_On_Reset > représente le champ **Resync On Reset**.
  - Chaque nom d'élément doit être unique. Dans les pages web d'administration, les mêmes champs peuvent apparaître sur plusieurs pages web, telles que les pages de ligne, d'utilisateur et de numéro de poste. Ajouter `[n]` au nom de l'élément pour indiquer le numéro affiché sur l'onglet de la page.

    Par exemple : l'élément <Dial_Plan_1_> représente le **Plan de numérotation** pour la ligne 1.
- À chaque balise d'ouverture de l'élément doit correspondre une balise de fermeture. Par exemple :

```
<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>
```

- Les balises d'éléments respectent la casse.
- Les balises d'élément vide sont autorisées et seront interprétées comme configurant la valeur à vide. Saisissez la balise d'ouverture de l'élément sans la balise d'élément correspondante et insérer un espace et une barre oblique avant le signe de fermeture (>). Dans cet exemple, la règle du profil B est vide :

```
<Profile_Rule_B />
```

- Une balise d'élément vide est utilisable pour empêcher le remplacement de toute valeur fournie par l'utilisateur lors de l'opération de resynchronisation. Dans l'exemple suivant, les paramètres de numérotation abrégée de l'utilisateur restent inchangées :

```
<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>
```

- Utilisez une valeur vide pour définir le paramètre correspondant à une valeur de chaîne vide. Saisissez un élément d'ouverture et de fermeture sans aucune valeur entre eux. Dans l'exemple suivant, le paramètre GPP_A est défini à une chaîne vide.

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

- Les noms d'élément non reconnus sont ignorés.

Rubriques connexes

Configuration du contrôle d'accès, à la page 9

Attribut d'accès utilisateur

Les commandes d'attribut d'accès utilisateur (**ua)** peuvent être utilisées pour modifier l'accès du compte d'utilisateur. Si l'attribut **ua** n'est pas spécifié, la configuration d'accès utilisateur existante est conservée. Cet attribut n'affecte par l'accès du compte d'administrateur.

L'attribut **ua** s'il est présent, doit avoir l'une des valeurs suivantes :

- na – pas d'accès
- ro – lecture seule
- rw – lecture/écriture

L'exemple suivant illustre l'attribut **ua** :

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

Des guillemets doubles doivent entourer la valeur de l'option **ua**.

Contrôle d'accès

Si le paramètre <Phone-UI-User-Mode> est activé, l'interface graphique du téléphone respecte l'attribut d'accès utilisateur des paramètres concernés lorsque l'interface graphique présente un élément du menu.

Pour les entrées du menu qui sont associées à un paramètre de configuration unique :

- La mise à disposition du paramètre avec l'attribut « ua=na » (« ua » signifie « accès utilisateur ») fait disparaître l'entrée.
- La mise à disposition du paramètre avec l'attribut « ua = ro » rend l'entrée en lecture seule et non modifiable.

Pour les entrées du menu qui sont associées à plusieurs paramètres de configuration :

- La mise à disposition de tous les paramètres concernés avec l'attribut « ua=na » fait disparaître les entrées.

Rubriques connexes

Configuration du contrôle d'accès, à la page 9

Propriétés des paramètres

Ces propriétés s'appliquent aux paramètres :

- Tous les paramètres qu'aucun profil ne précise demeurent inchangés dans le téléphone.
- Les paramètres non reconnus sont ignorés.
- Si le profil de format ouvert contient plusieurs occurrences de la même balise de paramètre, la dernière de ces occurrences a priorité sur les plus anciennes. Pour éviter d'écraser par inadvertance les valeurs de configuration d'un paramètre, il est recommandé que chaque profil précise au maximum une instance d'un paramètre.
- Le dernier profil traité est prioritaire. Si plusieurs profils spécifient le même paramètre de configuration, la valeur du profil le plus récent est prioritaire.

Formats de la chaîne

Ces propriétés s'appliquent au formatage des chaînes :

- Les commentaires sont autorisés via la syntaxe XML standard.

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

- Les espaces blancs et de fin sont autorisés pour améliorer la lisibilité, mais sont supprimés de la valeur du paramètre.
- Les nouvelles lignes au sein d'une valeur sont converties en espaces.
- Un en-tête XML sous la forme `<? ?>` est autorisé, mais le téléphone ne le prend pas en compte.
- Pour saisir des caractères spéciaux, utilisez des caractères XML d'échappement de base, comme indiqué dans le tableau suivant.

Caractère spécial	Séquence d'échappement XML
& (et commercial)	&
< (inférieur à)	<
> (supérieur à)	>
' (apostrophe)	'
« (double guillemet)	"

Dans l'exemple suivant, les caractères d'échappement sont saisis pour représenter les symboles supérieur à et inférieur à nécessaires dans une règle de plan de numérotation. Cet exemple définit un plan de numérotation de service téléphonique d'informations définissant le paramètre < Dial_Plan_1_> (**Connexion d'administration** > **Avancé** > **Voix** > **Poste (n)**)) égal à (S0 <:18005551212>).

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

- Les caractères numériques d'échappement, utilisent des valeurs décimales et hexadécimales (C'est-à-dire (et .), sont traduits.
- Le micrologiciel du téléphone ne prend en charge que des caractères ASCII.

Chiffrement et compression de profil ouvert (XML)

Le profil de configuration ouvert peut être compressé pour réduire la charge du réseau sur le serveur de configuration. Le profil peut également être chiffré pour assurer la protection des informations confidentielles. La compression n'est pas obligatoire, mais elle doit précéder le chiffrement.

Rubriques connexes

Formats de profil de configuration, à la page 15

Compression de profil ouvert

La méthode de compression prise en charge est l'algorithme de compression gzip (RFC1951). L'utilitaire gzip et la bibliothèque de compression qui mettent en œuvre le même algorithme (zlib) sont disponibles à partir de sites Internet.

Pour identifier la compression, le téléphone prévoit que le fichier compressé contienne un en-tête compatible gzip. L'appel de l'utilitaire gzip sur le profil ouvert d'origine génère l'en-tête. Le téléphone contrôle l'en-tête du fichier téléchargé pour déterminer le format de fichier.

Par exemple, si `profile.xml` est un profil valide, le fichier `profile.xml.gz` est également accepté. Une des commandes suivantes peut générer ce type de profil :

- `>gzip profile.xml`

  Remplace le fichier d'origine par le fichier compressé.

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

  Laisse le fichier d'origine en place, génère un nouveau fichier compressé.

Un didacticiel sur la compression est fourni à la section Compresser un profil ouvert avec Gzip, à la page 65.

Rubriques connexes

Compresser un profil ouvert avec Gzip, à la page 65

Chiffrement de profil ouvert

Le chiffrement par clé symétrique est utilisable pour chiffrer un profil de configuration ouvert, que le fichier soit compressé ou non. La compression, si elle est utilisée, doit être appliquée avant le chiffrement.

Le serveur de configuration utilise le protocole HTTPS pour traiter la mise à disposition initiale du téléphone après le déploiement. Le pré-chiffrement des profils de configuration hors connexion permet l'utilisation de HTTP pour synchroniser les profils. Cette fonctionnalité réduit la charge sur le serveur HTTPS dans les déploiements à grande échelle.

Le téléphone prend en charge deux méthodes de chiffrement pour les fichiers de configuration :

- Chiffrement AES-256-CBC

- Chiffrement du contenu HTTP en fonction de RFC-8188 avec un chiffrement AES-128-GCM

La clé ou information de saisie de clé (IKM) doit être mise à disposition par avance dans l'unité à une heure antérieure. Le démarrage de la clé secrète peut être réalisé en toute sécurité à l'aide de HTTPS.

Le nom de fichier final ne nécessite pas un format spécifique, mais un nom de fichier se terminant par l'extension `.cfg` indique normalement un profil de configuration.

Chiffrement AES-256-CBC

Le téléphone prend en charge le chiffrement AES-256-CBC pour les fichiers de configuration.

L'outil de chiffrement OpenSSL, disponible en téléchargement à partir de différents sites Internet, peut effectuer le chiffrement. La prise en charge pour le chiffrement AES 256 bits peut nécessiter la recompilation de l'outil pour activer le code AES. Le micrologiciel a été testé par rapport à la version openssl-0.9.7c.

Chiffrer un profil avec OpenSSL, à la page 66 propose un didacticiel sur le chiffrement.

Pour un fichier chiffré, le profil prévoit que le fichier aura le format généré par la commande suivante :

```
# 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
```

Un -k minuscule précède la clé secrète, qui peut être n'importe quelle phrase en texte non chiffré, et qui est utilisée pour générer une racine 64 bits aléatoire. Avec le mot de passe spécifié par l'argument -k, l'outil de chiffrement dérive un vecteur initial aléatoire 128 bits et la clé de chiffrement 256 bits réelle.

Lorsque cette forme de chiffrement est utilisée sur un profil de configuration, le téléphone doit connaître la valeur de la clé secrète pour déchiffrer le fichier. Cette valeur est spécifiée comme un identificateur dans l'URL du profil. La syntaxe est la suivante, à l'aide d'une URL explicite :

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

Cette valeur est programmée en appliquant l'un des paramètres Profile_Rule.

Rubriques connexes

Chiffrer un profil avec OpenSSL, à la page 66

Expansion de macro

Plusieurs paramètres de mise à disposition font l'objet d'une expansion de macro interne avant d'être évalués. Cette étape de pré-évaluation donne une plus grande souplesse de contrôle des activités de resynchronisation et de mise à niveau du téléphone.

Ces groupes de paramètres font l'objet d'expansion de macro avant l'évaluation :

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg

- Upgrade_Rule

Dans certaines conditions, certains paramètres généraux (GPP _*) sont soumis à une expansion de macro, comme explicitement indiqué en Arguments de resynchronisation facultatifs, à la page 25.

Au cours de l'expansion de macro, le contenu des variables nommées remplace des expressions de la forme $NAME et $(NAME). Ces variables incluent des paramètres généraux, plusieurs identificateurs de produit, certains minuteurs d'événement et les valeurs d'état de mise à disposition. Pour en obtenir la liste complète, consultez Variables d'expansion de macro, à la page 79.

Dans l'exemple suivant, l'expression $(MAU) est utilisée pour insérer l'adresse MAC 000E08012345.

L'administrateur saisit : **`$(MAU)config.cfg`**

L'expansion de macro résultante pour un périphérique ayant l'adresse MAC 000E08012345 est : `000E08012345config.cfg`

Si un nom de macro n'est pas reconnu, il demeure non étendu. Par exemple, le nom STRANGE n'est pas reconnu comme nom de macro valide, tandis que MAU est considéré comme un nom de macro valide.

L'administrateur saisit : **`$STRANGE$MAU.cfg`**

L'expansion de macro résultante pour un périphérique ayant l'adresse MAC 000E08012345 est : `$STRANGE000E08012345.cfg`

L'expansion de macro n'est pas appliquée de manière récursive. Par exemple, $$MAU” est développé en $MAU” (le $$ est développé) et ne se traduit pas par l'adresse MAC.

Le contenu des paramètres à usages spéciaux, GPP_SA à GPP_SD, est mis en correspondance avec les expressions macro $SA à $SD. Ces paramètres subissent uniquement une expansion de macro en tant qu'argument des options de la **--key**, **--uid** et **--pwd** dans une URL de resynchronisation.

Expressions conditionnelles

Les expressions conditionnelles peuvent déclencher des événements de resynchronisation à partir de l'URL de remplacement dans le cas des opérations de resynchronisation et de mise à niveau.

Les expressions conditionnelles se composent d'une liste de comparaisons, séparées par l'opérateur **et**. Toutes les comparaisons doivent être satisfaites pour que la condition soit vraie.

Chaque comparaison peut se rapporter à un des trois types d'opérandes suivants :

- Valeurs entières
- Numéros de version de logiciel ou de matériel
- Chaînes entre guillemets doubles

Numéros de version

La version logicielle officielle des téléphones multiplateformes (MPP) utilise ce format, où BN == Numéro de version:

- Téléphone IP Cisco 6800 Series :`sip68xx.v1-v2-v3MPP-BN`

La chaîne de comparaison doit utiliser le même format. Dans le cas contraire, un erreur d'analyse de format se produit.

Dans la version du logiciel, v1-v2-v3-v4 peut désigner différents chiffres et caractères, mais doit commencer par un chiffre. Lorsque vous comparez la version du logiciel, v1-v2-v3-v4 est comparée dans l'ordre et les chiffres les plus à gauche sont prioritaires sur les derniers.

Si v [x] ne comprend que des chiffres, les chiffres sont comparés ; si v [x] inclut des chiffres + caractères alphabétiques, les chiffres sont comparés d'abord, puis les caractères sont comparés dans l'ordre alphabétique.

Exemple de numéro de version valide

sipyyyy.11-0-0MPP-BN

À l'inverse : 11.0.0 est un format non valide.

Comparaison

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

Les chaînes entre guillemets peuvent être comparées pour leur égalité ou leur inégalité. Les numéros de version et les nombres entiers peuvent également être comparés. Les opérateurs de comparaison peuvent être exprimés sous forme de symboles ou d'acronymes. Les acronymes sont utiles pour l'expression de la condition dans un profil de format ouvert.

Opérateur	Autre syntaxe	Description	Applicable aux opérandes entiers et numéros de version	Applicable aux opérandes de chaînes entre guillemets
=	eq	égal à	Oui	Oui
!=	ne	non égal à	Oui	Oui
<	lt	inférieur à	Oui	Non
<=	ie	inférieur ou égal à	Oui	Non
>	gt	supérieur à	Oui	Non
>=	se	supérieur ou égal à	Oui	Non
ET		et	Oui	Oui

Il est important d'encadrer les variables de macro de guillemets là où une chaîne littérale est attendue. Ne le faites pas lorsqu'un numéro ou un numéro de version sont attendus.

Lorsqu'elles sont utilisées dans le cadre des paramètres Profile_Rule* et Upgrade_Rule, les expressions conditionnelles doivent être placées dans la syntaxe « (expression) ? », comme dans cet exemple de règle de mise à niveau. N'oubliez pas que BN signifie le numéro de version.

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

N'utilisez pas la syntaxe précédente avec des parenthèses pour configurer les paramètres Resync_Trigger_*.

Syntaxe des URL

Utilisez la syntaxe des URL standard pour indiquer comment récupérer les micrologiciels et les fichiers de configuration dans les paramètres Profile_Rule* et Upgrade_Rule, respectivement. La syntaxe est la suivante :

Chemin [schéma://] [serveur [:port]]

Où **schéma** prend l'une des valeurs suivantes :

- tftp
- http
- HTTPS

Si **schéma** est omis, par défaut tftp est utilisé. Le serveur peut être un nom d'hôte DNS reconnu ou une adresse IP numérique. Le port est le numéro de port TCP ou UDP de destination. Le chemin d'accès doit commencer par le répertoire racine (/) ; Il doit être un chemin d'accès absolu.

Si **serveur** est manquant, le serveur tftp spécifié via DHCP (option 66) est utilisé.

Remarque Pour les règles de mise à niveau, le serveur doit être spécifié.

Si **port** est manquant, le port standard pour le schéma spécifié est utilisé. Tftp utilise le port UDP 69, http utilise le port TCP 80, https utilise le port TCP 443.

Un chemin d'accès doit être présent. Il ne doit pas nécessairement faire référence à un fichier statique, mais peut indiquer un contenu dynamique obtenu au moyen de CGI.

L'expansion de macro s'applique au sein des URL. Voici des exemples d'URL valides :

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

Lorsque vous utilisez l'option DHCP 66, la syntaxe vide n'est pas prise en charge par les règles de mise à niveau. Elle ne s'applique qu'à Profile_Rule*.

Chiffrement du contenu HTTP en fonction de RFC-8188

Le téléphone prend en charge le chiffrement du contenu HTTP en fonction de RFC 8188 avec un chiffrement AES-128-GCM des fichiers de configuration. Avec cette méthode de codage, toutes les entités peuvent lire les en-têtes de message HTTP. Cependant, seules les entités qui connaissent l'IKM (Input Keying Material, Informations de saisie d'entrée) peuvent lire la charge utile. Lorsque le téléphone est mis à disposition avec l'IKM, le téléphone et le serveur de mise à disposition peuvent échanger des fichiers de configuration en toute sécurité, tout en autorisant les éléments du réseau de fabricants tiers à utiliser les en-têtes de messages à des fins d'analyse et de surveillance.

Le paramètre de configuration XML **IKM_HTTP_Encrypt_Content** contient l'IKM sur le téléphone. Pour des raisons de sécurité, ce paramètre n'est pas accessible sur la page web d'administration du téléphone. Il n'est pas non plus visible dans le fichier de configuration du téléphone, auquel vous pouvez accéder à partir de l'adresse IP du téléphone ou depuis les rapports de configuration du téléphone envoyés au serveur de mise à disposition.

Si vous souhaitez utiliser le chiffrement RFC 8188, assurez-vous que vous :

- Configurez le téléphone avec IKM en spécifiant l'IKM avec le paramètre XML **IKM_HTTP_Encrypt_Content** dans le fichier de configuration qui est envoyé du serveur de mise à disposition au téléphone.
- Si ce chiffrement est appliqué aux fichiers de configuration transmis à partir du serveur de mise à disposition au téléphone, vérifiez que l'en-tête HTTP de *codage de contenu* dans le fichier de configuration comporte « aes128gcm ».

  En l'absence de cet en-tête, la méthode AES-256-CBC est prioritaire. Le téléphone applique le déchiffrement AES-256-CBC si une clé AES-256-CBC est présente dans une règle de profil, sans tenir compte de IKM.
- Si vous souhaitez que le téléphone applique ce chiffrement à la configuration des rapports qu'il envoie au serveur de mise à disposition, vérifiez qu'aucune clé AES-256-CBC n'est spécifiée dans la règle de rapport.

Arguments de resynchronisation facultatifs

Les arguments facultatifs, **key**, **uid**, et **pwd**, peuvent précéder les URL saisies dans les paramètres Profile_Rule*, collectivement placés entre crochets.

key

L'option **--key** indique au téléphone que le fichier de configuration qu'il reçoit à partir du serveur de mise à disposition est chiffré avec le chiffrement AES-256-CBC, sauf si l'en-tête de *codage de contenu* dans le fichier indique un chiffrement « aes128gcm ». La clé elle-même est spécifiée comme une chaîne suivant le terme **--key**. Vous pouvez placer la clé de chiffrement entre guillemets doubles (") de manière optionnelle. Le téléphone utilise la clé pour déchiffrer le fichier de configuration.

Exemples d'utilisation

```
[--key VerySecretValue]
[--key “my secret phrase”]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

Les arguments facultatifs entre crochets font l'objet d'une expansion de macro. Les paramètres à usage spécial, GPP_SA à GPP_SD, font l'objet d'expansion de macro en variables macro, $SA à $SD, uniquement lorsqu'ils sont utilisés comme arguments facultatifs de la clé. Consultez ces exemples :

```
[--key $SC]
[--key “$SD”]
```

Dans les profils de format ouverts, l'argument de **-key** doit être identique à l'argument facultatif de **-k** fourni à **openssl**.

ID utilisateur et mot de passe

Les options **uid** et **pwd** peuvent être utilisées pour indiquer l'ID utilisateur et le mot de passe pour l'URL spécifiée. Les arguments facultatifs entre crochets font l'objet d'une expansion de macro. Les paramètres à usage spécial, GPP_SA à GPP_SD, font l'objet d'expansion de macro en variables macro, $SA à $SD, uniquement lorsqu'ils sont utilisés comme arguments facultatifs de la clé. Consultez ces exemples :

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

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

Une fois étendus deviennent :

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

Appliquer un profil au périphérique de téléphonie IP

Après avoir créé un script de configuration XML, il doit être transmis au téléphone pour application. Pour appliquer la configuration, vous pouvez soit télécharger le fichier de configuration sur le téléphone à partir d'un serveur TFTP, HTTP ou HTTPS à l'aide d'un navigateur web, soit utiliser l'utilitaire de ligne de commande cURL.

Télécharger le fichier de configuration sur le téléphone à partir d'un serveur TFTP

Procédez comme suit pour télécharger le fichier de configuration d'une application du serveur TFTP sur votre PC.

Procédure

Étape 1 Connectez votre ordinateur au LAN du téléphone.

Étape 2 Exécutez une application de serveur TFTP sur le PC et assurez-vous que le fichier de configuration est disponible dans le répertoire racine TFTP.

Étape 3 Dans un navigateur web, saisissez l'adresse IP du réseau local du téléphone, l'adresse IP de l'ordinateur, le nom de fichier et les informations de connexion. Utilisez ce format :

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

Exemple :

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

Téléchargez le fichier de configuration sur le téléphone IP avec cURL

Procédez comme suit pour télécharger la configuration sur le téléphone à l'aide de cURL. Cet outil de ligne de commande est utilisé pour transférer des données avec une syntaxe d'URL. Pour télécharger cURL, consultez :

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

Remarque Il est recommandé que vous n'utilisiez pas cURL pour valider la configuration jusqu'au téléphone, car le nom d'utilisateur et le mot de passe peuvent être cURL

Procédure

Étape 1 Connectez votre PC au port LAN du téléphone.

Étape 2 Téléchargez le fichier de configuration sur le téléphone en saisissant la commande suivante cURL :

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

Paramètres de mise à disposition

Cette section décrit les paramètres de mise à disposition organisés dans une large mesure par rapport à une fonction :

Ces types de paramètres de mise à disposition existent :

- Objectif général
- Enables
- Déclenchements
- Horaires configurables
- Règles de profil
- Règle de mise à niveau

Paramètres généraux

Les paramètres d'usage général GPP _* (**Connexion d'administration** > **Avancé** > **Voix** > **Mise à disposition**) sont utilisés comme registres de chaîne libre, lors de la configuration du téléphone pour interagir avec une solution de serveur de mise à disposition donnée. Les paramètres GPP _* sont vides par défaut. Ils peuvent être configurés pour obtenir diverses valeurs, notamment les suivantes :

- Clés de chiffrement.
- URL

- Informations sur l'état d'une mise à disposition en plusieurs étapes
- Modèles de requête de publication
- Mappages d'alias de noms de paramètres.
- Des valeurs de chaîne partielles, pouvant être combinées en des valeurs de paramètre complètes.

Les paramètres GPP _* sont disponibles pour l'expansion de macro au sein d'autres paramètres de mise à disposition. À cette fin, les noms de macros en majuscules avec une seule lettre (A-P) suffisent pour identifier le contenu du GPP_A au GPP_P. En outre, les noms de macros en majuscules à deux lettres SA à SD identifient GPP_SA à GPP_SD comme un cas particulier lorsqu'ils sont utilisés comme arguments des options URL suivantes :

key, **uid**, et **pwd**

Ces paramètres peuvent être utilisés en tant que variables dans les règles de mise à disposition et mise à niveau. Ils sont référencés en préfixant le nom de la variable par un caractère '$', comme $GPP_A.

Utiliser des paramètres généraux

Par exemple, si GPP_A contient la chaîne ABC et GPP_B contient 123, la macro de l'expression AB est développée en ABC123.

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Sélectionnez **Voix** > **Mise à disposition**.

Étape 2 Faites défiler jusqu'à la section **Paramètres à usage général**.

Étape 3 Saisissez des valeurs valides dans les champs, A GPP à GPP P.

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Enables

Les paramètres Provision_Enable et Upgrade_Enable contrôlent toutes les resynchronisations de profil et opérations de mise à niveau du micrologiciel. Ces paramètres contrôlent les resynchronisations et les mises à niveau indépendamment. Ces paramètres contrôlent également les commandes de resynchronisation et de mise à niveau qui sont émises par le serveur web d'administration. Ces deux paramètres sont définis sur **Oui** par défaut.

Le paramètre Resync_From_SIP contrôle les requêtes de resynchronisation. Un événement SIP NOTIFY est envoyé à partir du serveur de proxy du fournisseur de services au téléphone. S'il est activé, le proxy peut demander une resynchronisation. Pour ce faire, le serveur proxy envoie un message SIP NOTIFY contenant l'événement : en-tête de resynchronisation, au périphérique.

Le périphérique répond à la requête avec une réponse 401 (autorisation refusée pour les informations d'identification utilisées). Le périphérique attend une requête ultérieure authentifiée avant d'exécuter la requête

de resynchronisation du proxy. Les en-têtes d'événement : reboot_now et : restart_now effectuent des redémarrages à froid et à chaud, respectivement, qui sont également validés par le serveur.

Les deux derniers paramètres Enables sont Resync_On_Reset et Resync_After_Upgrade_Attempt. Ces paramètres déterminent si le périphérique effectue une opération de resynchronisation après la séquence d'amorçage du logiciel et après chaque tentative de mise à niveau.

Lorsque Resync_On_Reset est activé, le périphérique introduit un délai aléatoire qui suit la séquence d'amorçage avant d'effectuer la réinitialisation. Le délai est une durée aléatoire jusqu'à la valeur indiquée par le paramètre Resync_Random_Delay (en secondes). Dans un pool de téléphones qui se mettent en marche simultanément, ce délai permet de répartir les heures de début des demandes de resynchronisation de chaque unité. Cette fonctionnalité peut être utile dans les déploiements résidentiels de grande envergure, en cas de panne d'électricité régionale.

Déclenchements

Le téléphone permet la resynchronisation à des intervalles spécifiques ou à une heure donnée.

Resynchroniser à des intervalles spécifiques

Le téléphone est conçu pour se resynchroniser régulièrement avec le serveur de mise à disposition. L'intervalle de resynchronisation est configuré dans Resync_Periodic (en secondes). Si cette valeur est laissée vide, ou si elle est égale à zéro, le périphérique n 'est pas resynchronisé périodiquement.

La resynchronisation a généralement lieu lorsque les lignes téléphoniques sont inactives. Lorsqu'une ligne vocale est active et qu'une resynchronisation doit avoir lieu, le téléphone retarde la resynchronisation jusqu'à ce que la ligne redevienne inactive. Une resynchronisation peut entraîner la modification des valeurs des paramètres de configuration.

Une resynchronisation peut échouer parce que le téléphone ne parvient pas à récupérer un profil à partir du serveur, parce que le fichier téléchargé est endommagé, ou parce qu'une erreur interne s'est produite. Le périphérique tente d'effectuer une resynchronisation à nouveau après une durée spécifiée dans Resync_Error_Retry_Delay (en secondes). Si Resync_Error_Retry_Delay est défini sur 0, le périphérique ne tente pas d'effectuer à nouveau une resynchronisation après une tentative de resynchronisation infructueuse.

Si une mise à niveau échoue, une nouvelle tentative est effectuée après Upgrade_Error_Retry_Delay secondes.

Deux paramètres configurables sont disponibles pour déclencher sous condition une resynchronisation : Resync_Trigger_1 et Resync_Trigger_2. Chaque paramètre peut être programmé avec une expression conditionnelle qui subit une expansion de macro. À l'expiration de l'intervalle de resynchronisation (heure de la prochaine resynchronisation) les déclencheurs, s'ils ont été définis, empêchent la resynchronisation, sauf si un au moins des déclencheurs est égal à Vrai.

L'exemple de condition suivant déclenche une resynchronisation. Dans cet exemple, la dernière tentative de mise à niveau de téléphone s'est écoulée il y a plus de 5 minutes (300 secondes), et moins de 10 minutes (600 secondes) se sont écoulées depuis la dernière tentative de resynchronisation.

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

Resynchronisation à une heure donnée

Le paramètre Resync_At permet au téléphone de se resynchroniser à une heure donnée. Ce paramètre utilise le format 24 heures (hhmm) pour spécifier l'heure.

Le paramètre Resync_At_Random_Delay permet au téléphone d'effectuer une resynchronisation après un délai non spécifié dans le temps. Ce paramètre utilise un format entier positif pour indiquer l'heure.

Saturer le serveur avec des requêtes de resynchronisation de plusieurs téléphones qui sont configurés pour effectuer une resynchronisation en même temps doit être évité. Pour ce faire, le téléphone déclenche la resynchronisation au maximum 10 minutes après l'heure spécifiée.

Par exemple, si vous définissez l'heure de resynchronisation à 1000 (10 h 00), le téléphone déclenchera la resynchronisation à tout instant entre 10 h 00 et 10 h 10

Cette fonctionnalité est désactivée par défaut. Lorsque le paramètre Resync_At est mis à disposition, le paramètre Resync_At est ignoré.

Horaires configurables

Vous pouvez configurer des horaires de resynchronisations périodiques, et vous pouvez spécifier des intervalles de nouvelle tentative en cas d'échec de resynchronisation et de mise à niveau à l'aide de ces paramètres de mise à disposition :

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

Chaque paramètre accepte un seul délai (en secondes). La nouvelle syntaxe étendue permet une liste séparée par des virgules des délais consécutifs. Le dernier élément de la séquence est répété implicitement de manière continue.

Éventuellement, vous pouvez utiliser un signe plus pour indiquer une valeur numérique qui ajoute un délai aléatoire supplémentaire, comme illustré dans cet exemple.

Exemple 1

Dans cet exemple, le téléphone effectue périodiquement une resynchronisation toutes les 2 heures. En cas de panne de resynchronisation, le périphérique effectue une nouvelle tentative à ces intervalles : 30 minutes, 1 heure, 2 heures, 4 heures. Le périphérique continue d'essayer à des intervalles de 4 heures jusqu'à ce qu'il se resynchronise avec succès.

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

Exemple 2

Dans cet exemple, le périphérique se resynchronise périodiquement toutes les heures (plus un délai supplémentaire aléatoire de 10 minutes). Dans le cas d'une panne de resynchronisation, le périphérique effectue une nouvelle tentative à ces intervalles : 30 minutes (plus 5 minutes au maximum). 1 heure (plus 10 minutes au maximum), 2 heures (plus jusqu'à 15 minutes). Le périphérique continue d'essayer à des intervalles de 2 heures (plus 15 minutes au maximum) jusqu'à ce qu'il se resynchronise avec succès.

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

Exemple 3

Dans cet exemple, si une tentative de mise à niveau à distance échoue, le périphérique retente la mise à niveau au bout de 30 minutes, puis à nouveau après une heure, puis dans deux heures. Si la mise à niveau échoue, le périphérique effectue une nouvelle tentative toutes les quatre à cinq heures jusqu'à ce que la mise à niveau réussisse.

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

Règles de profil

Le téléphone fournit plusieurs paramètres de profil de configuration à distance (Profile_Rule*). C'est pourquoi, chaque opération de resynchronisation peut récupérer plusieurs fichiers, gérés par des serveurs distincts.

Dans le scénario le plus simple, le périphérique se resynchronise périodiquement à un seul profil sur un serveur principal, qui met à jour tous les paramètres internes qui s'appliquent. Le profil peut aussi être partagé entre différents fichiers. Un seul fichier est commun à tous les téléphones d'un déploiement. Un fichier distinct, unique est fourni pour chaque compte. Les clés de chiffrement et les informations de certificat peuvent être fournies par encore un autre profil, stocké sur un serveur distinct.

Chaque fois qu'une resynchronisation doit être effectuée, le téléphone évalue les quatre paramètres Profile_Rule* dans l'ordre :

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

Chaque évaluation peut entraîner une récupération du profil à partir d'un serveur de mise à disposition à distance, avec une mise à jour possible d'un certain nombre de paramètres internes. Si une évaluation échoue, la séquence de resynchronisation est interrompue et est retentée à nouveau au moment spécifié par le paramètre Resync_Error_Retry_Delay (en secondes). Si toutes les évaluations réussissent, le périphérique attend la seconde spécifiée par le paramètre Resync_Periodic et exécute ensuite un autre resynchronisation.

Le contenu de chaque paramètre Profile_Rule* se compose d'un ensemble de solutions alternatives. Les solutions alternatives sont séparées par le caractère | (barre verticale). Chaque solution alternative se compose d'une expression conditionnelle, d'une expression d'affectation, d'une URL de profil et de toutes les options d'URL associées. Tous ces composants sont facultatifs au sein de chaque alternative. Voici les combinaisons valides et l'ordre dans lequel elles doivent s'affichent, le cas échéant :

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

Au sein de chaque paramètre Profile_Rule*, toutes les solutions alternatives sauf la dernière, doivent fournir une expression conditionnelle. Cette expression est évaluée et est traitée comme suit :

1. Les conditions sont évaluées de gauche à droite, jusqu'à ce qu'il en existe une qui donne la valeur Vrai (ou jusqu'à ce qu'une alternative soit trouvée sans expression conditionnelle).
2. Toutes les expressions d'affectation d'accompagnement sont évaluées, le cas échéant.

3. Si une URL est spécifiée dans le cadre de cette solution alternative, une tentative est effectuée pour télécharger le profil qui se trouve à l'URL spécifiée. Le système tente de mettre à jour les paramètres internes en conséquence.

Si toutes les alternatives comportent des expressions conditionnelles et qu'aucune ne prend la valeur Vrai (ou si l'ensemble de la règle du profil est vide), le paramètre Profile_Rule* tout entier est ignoré. Le paramètre de règle de profil suivant de la séquence est évalué.

Exemple 1

Cet exemple effectue une resynchronisations inconditionnelle au profil de l'URL spécifiée et une requête HTTP GET au serveur de mise à disposition à distance :

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

Exemple 2

Dans cet exemple, le périphérique effectue une resynchronisation à deux URL différentes, selon l'état de l'enregistrement de la ligne 1. En cas d'enregistrement perdu, le périphérique effectue un HTTP POST vers un script CGI. Le périphérique envoie le contenu de la macro étendue GPP_A, qui peut fournir des informations supplémentaires sur l'état du périphérique :

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

Exemple 3

Dans cet exemple, le périphérique réalise une resynchronisation sur le même serveur. Le périphérique fournit des informations supplémentaires, si un certificat n'est pas installé sur l'unité (pour les unités antérieures à la 2.0 existantes) :

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

Exemple 4

Dans cet exemple, la ligne 1 est désactivée jusqu'à ce que GPP_A soit défini comme égal à Mis à disposition par la première URL. Ensuite, il effectue une resynchronisation à la deuxième URL :

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

Exemple 5

Dans cet exemple, on suppose que le profil que le serveur renvoie contient des balises d'éléments XML. Ces balises doivent être mappées de nouveau aux noms de paramètres appropriés par la correspondance des alias stockée dans GPP_B :

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

Une resynchronisation est généralement considérée comme ayant échoué si un profil demandé n'est pas reçu du serveur. Le paramètre Resync_Fails_On_FNF peut remplacer ce comportement par défaut. Lorsque Resync_Fails_On_FNF est défini sur Non, le périphérique considère la réponse file-not-found du serveur comme une resynchronisation réussie. La valeur par défaut pour Resync_Fails_On_FNF est Oui.

Règle de mise à niveau

La règle de mise à niveau informe le périphérique qu'il doit s'activer pour recevoir une nouvelle charge et d'où obtenir la charge, le cas échéant. Si la charge est déjà sur le périphérique, il ne tente pas d'obtenir la charge. Ainsi, la validité de l'emplacement de charge importe peu lorsque la charge souhaitée se trouve dans la partition inactive.

L'Upgrade_Rule indique une version de micrologiciel qui, si elle est différente de la charge actuelle, est téléchargée et appliquée à moins qu'elle ne soit limitée par une expression conditionnelle ou que Upgrade_Enable soit défini sur **Non**.

Le téléphone fournit un paramètre de mise à niveau configurable à distance, Upgrade_Rule. Ce paramètre accepte une syntaxe similaire aux paramètres de règle de profil. Les options d'URL ne sont pas prises en charge pour les mises à niveau, mais les expressions conditionnelles et les expressions d'affectation peuvent être utilisées. Si des expressions conditionnelles sont utilisées, le paramètre peut être rempli avec plusieurs alternatives, séparées par le caractère |. La syntaxe de chaque alternative est la suivante :

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

Comme dans le cas des paramètres de Profile_Rule*, le paramètre Upgrade_Rule évalue chaque alternative jusqu'à ce qu'une expression conditionnelle soit satisfaite ou qu'une alternative ne comporte aucune expression conditionnelle. L' expression d'affectation d'accompagnement est évaluée, le cas échéant. Puis, une tentative de mise à niveau vers l'URL spécifiée est effectuée.

Si Upgrade_Rule contient une URL sans expression conditionnelle, le périphérique est mis à niveau vers l'image du micrologiciel que spécifie l'URL. Après l'expansion de macro et l'évaluation de la règle, le périphérique n'effectue pas une nouvelle tentative de mise à niveau jusqu'à ce que la règle soit modifiée ou que la combinaison schéma + serveur + port + chemin d'accès soit modifiée.

Pour tenter une mise à niveau du micrologiciel, le périphérique désactive l'audio au début de la procédure et le redémarre à la fin de la procédure. Le périphérique ne démarre automatiquement une mise à niveau qui est définie par le contenu de Upgrade_Rule que si toutes les lignes téléphoniques sont actuellement inactives.

Par exemple,

- Dans le cas du téléphone IP Cisco 6800 Series :

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

  where BN==Build Number
  ```

Dans cet exemple, Upgrade_Rule met à niveau le micrologiciel vers l'image qui est stockée à l'adresse indiquée.

Voici un autre exemple concernant le téléphone IP Cisco 6800 Series :

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

where BN==Build Number
```

Cet exemple indique à l'unité de charger l'une des deux images, en fonction du contenu du paramètre général, GPP_F.

Le périphérique peut imposer une limite antérieure concernant le numéro de révision du micrologiciel, ce qui peut être une option de personnalisation utile. Si un numéro de révision du micrologiciel valide est configuré dans le paramètre Downgrade_Rev_Limit, le périphérique rejette les tentatives de mise à niveau pour les versions d'image antérieures à la limite spécifiée.

Types de données

Ces types de données sont utilisés avec les paramètres de profil de configuration :

- {a, b, c,...} : à choisir parmi a, b, c,...
- Boolean : valeur booléenne « Oui » ou « Non ».
- CadScript : un miniscript qui spécifie les paramètres de cadence d'un signal. Jusqu'à 127 caractères

  Syntaxe : S_1[; S_2], où :

  - S_i= D_i(activé$_{i,\ 1}$/ désactivé$_{i,\ 1}$[activé$_{i,\ 2}$/ désactivé$_{i,\ 2}$[activé$_{i,\ 3}$/ désactivé$_{i,\ 3}$[activé$_{i,\ 4}$/ désactivé$_{i,\ 4}$[activé$_{i,\ 5}$/ désactivé$_{i,\ 5}$[activé$_{i,\ 6}$/ désactivé$_{i,\ 6}$]]]]]) et est appelé une section.
  - activé$_{i,\ j}$ et désactivé$_{i,\ j}$ sont les durées en secondes activées/désactivées d'un *segment*.i = 1 ou 2 et j = 1 à 6.
  - D_i est la durée totale de la section en secondes.

  Toutes les durées peuvent posséder jusqu'à trois décimales pour fournir une résolution à 1 ms. Le caractère de remplacement « * » désigne une durée infinie. Les segments d'une section sont émis dans l'ordre et répétés jusqu'à la fin de la durée totale.

  Exemple 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
```

  Exemple 2 : sonnerie distincte (court, court, court, long) :

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

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

Total Ring Length = 60s
```

- DialPlanScript : la syntaxe de script qui est utilisée pour spécifier les plans de numérotation de la ligne 1 et de la ligne 2.
- Virgule flottante< n > : valeur avec virgule flottante comportant jusqu'à n décimales.
- FQDN : nom de domaine complet. Ce script peut atteindre 63 caractères. Voici quelques exemples :
  - sip.Cisco.com:5060 or 109.12.14.12:12345
  - sip.Cisco.com or 109.12.14.12
- FreqScript : un miniscript qui spécifie les paramètres de fréquence et de niveau d'une tonalité. Comprend jusqu'à 127 caractères.

  Syntaxe : $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, où :
  - $F_1 – F_6$ sont des fréquences en Hz (uniquement un entier non signé).
  - $L_1 – L_6$ sont les niveaux correspondant en décibels (dB) (comporte au maximum une décimale).

  Les espaces avant et après la virgule sont autorisés, mais non recommandés.

  Exemple 1 : tonalité d'attente d'appel :

```
440@-10

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

  Exemple 2 : tonalité :

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

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

- IP : adresse IPv4 sous la forme x.x.x.x, où x est compris entre 0 et 255. Exemple : 10.1.2.100.
- ID utilisateur : ID utilisateur tel qu'il apparaît dans une URL ; jusqu'à 63 caractères.
- Téléphone : une chaîne de numéro de téléphone, telle que 14081234567, *69, *72, 345678 ; ou une URL générique, par exemple, 1234@10.10.10.100:5068 ou jsmith@Cisco.com. La chaîne peut contenir jusqu'à 39 caractères.
- PhTmplt : un modèle de numéro de téléphone. Chaque modèle peut contenir un ou plusieurs modèles qui sont séparés par une virgule (,). Les espaces au début de chaque modèle sont ignorés. « ? » et « * » représentent des caractères génériques. Pour une représentation littérale, utilisez %xx. Par exemple, %2a représente *. Le modèle peut contenir jusqu'à 39 caractères. Exemples : “1408*, 1510*”, “1408123????, 555?1.”.
- Port : numéro de Port TCP/UDP (0 à 65535). Il peut être spécifié au format décimal ou hexadécimal.
- ProvisioningRuleSyntax : la syntaxe de script utilisée pour définir la resynchronisation de la configuration et les règles de mise à niveau du micrologiciel.
- PwrLevel : niveau d'alimentation exprimé en dBm avec une décimale, par exemple –13.5 ou 1,5 dBm.

- RscTmplt : un modèle de Code d'état de réponse SIP, par exemple « “404, 5*”, “61?”, “407, 408, 487, 481”. Ce script peut atteindre 39 caractères.
- Sig< n > : valeur signée n-bits. Elle peut être spécifiée au format décimal ou hexadécimal. Un signe « - » doit précéder les valeurs négatives. Un signe + précédant les valeurs positives est facultatif.
- Codes étoile : le code d'activation d'un service supplémentaire, par exemple *69. Le code peut contenir jusqu'à 7 caractères.
- Str< n > : une chaîne générique comportant jusqu'à n caractères non réservés.
- Time< n > : durée en secondes, comportant jusqu'à n décimales. Les décimales supplémentaires spécifiées sont ignorées.
- ToneScript : un mini-script qui détermine les paramètres de fréquence, de niveau et de cadence d'une tonalité de progression d'appel. Le script peut contenir jusqu'à 127 caractères.

  Syntaxe : FreqScript;Z_1[;Z_2].

  La section Z_1 est similaire à la section S_1 d'un CadScript, sauf que chaque segment activé/désactivé est suivi d'un paramètre de composants de fréquence : $Z_1 = D_1$(activé$_{i,1}$/ désactivé $_{i,1}$/$f_{i,1}$[activé$_{i,2}$/ désactivé$_{i,2}$/$f_{i,2}$ [activé$_{i,3}$/ désactivé$_{i,3}$/$f_{i,3}$ [, activé$_{i,4}$/ désactivé$_{i,4}$/$f_{i,4}$ [activé$_{i,5}$/ désactivé$_{i,5}$/$f_{i,5}$ [activé$_{i,6}$/ désactivé$_{i,6}$/$f_{i,6}$]]]]]) où :

  - $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$.
  - $1 < n_k < 6$ spécifie les composants de fréquence du FreqScript qui sont utilisés dans ce segment.

  Si plus d'un composant de fréquence est utilisé dans un segment, les composants sont additionnés.

  Exemple 1 : tonalité :

```
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
```

  Exemple 2 : tonalité à répétition :

```
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 > : valeur n bits non signée, où n = 8, 16 ou 32. Il peut être spécifié au format décimal ou hexadécimal, par exemple 12 ou 0x18, tant que la valeur peut s'adapter à ces n bits.

Remarque Gardez à l'esprit :

- < nom du param> représente un nom de paramètre de configuration. Dans un profil, la balise correspondante est formée en remplaçant l'espace par un trait de soulignement « _ », par exemple **Par_Name**.
- Un champ de valeur par défaut vide implique une chaîne vide < «» >.
- Le téléphone continue d'utiliser les dernières valeurs configurées pour les balises qui ne sont pas présentes dans un profil donné.
- Les modèles sont comparés dans l'ordre indiqué. La première, *et non la plus proche*, correspondance est sélectionnée. Le nom du paramètre doit correspondre exactement.
- Si plus d'une définition d'un paramètre est indiquée dans un profil, la dernière définition du fichier est celle qui est appliquée dans le téléphone.
- Une spécification de paramètre avec une valeur de paramètre vide force le paramètre à sa valeur par défaut. Pour spécifier une chaîne vide au lieu de cela, utilisez une chaîne vide «» en tant que valeur du paramètre.

Mises à jour de profil et mises à niveau du micrologiciel

Le téléphone prend en charge la mise à disposition à distance sécurisée (configuration) et les mises à niveau du micrologiciel. Un téléphone non mis à disposition peut recevoir un profil chiffré destiné à ce périphérique. Le téléphone ne nécessite pas de clé explicite en raison d'un mécanisme de première mise à disposition sécurisé qui utilise la fonctionnalité SSL.

L'intervention de l'utilisateur n'est pas nécessaire pour démarrer ou effectuer une mise à jour de profil, ou une mise à niveau du micrologiciel, ou si des mises à niveau intermédiaires sont nécessaires pour atteindre un état de mise à niveau postérieur à partir d'une version antérieure. Une resynchronisation du profil n'est retentée que lorsque le téléphone IP Cisco est inactif, car une resynchronisation peut déclencher un redémarrage du logiciel et mettre fin à un appel.

Les paramètres généraux gèrent le processus de mise à disposition. Tous les téléphones peuvent être configurés pour contacter régulièrement un serveur de mise à disposition normale (NPS). La communication avec le serveur de mise à disposition normale ne nécessite pas l'utilisation d'un protocole sécurisé car le profil mis à jour est crypté par une clé secrète partagée. Le serveur NPS peut être un serveur TFTP, HTTP ou HTTPS standard avec des certificats clients.

L'administrateur peut mettre à niveau, redémarrer, ou resynchroniser les téléphones à l'aide de l'interface utilisateur web du téléphone. L'administrateur peut également effectuer ces tâches à l'aide d'un message de notification SIP.

Les profils de configuration sont générés à l'aide d'outils open source communs qui s'intègrent aux systèmes de mise à disposition des prestataires de services.

Rubriques connexes

Autoriser et configurer les mises à jour du profil, à la page 38

Autoriser et configurer les mises à jour du profil

Des mises à jour du profil peuvent être autorisées à intervalles réguliers. Les profils mis à jour sont envoyés à partir d'un serveur sur le téléphone à l'aide de TFTP, HTTP ou HTTPS.

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Sélectionnez **Voix -** > **Mise à disposition**.

Étape 2 Dans la section **Profil de configuration**, sélectionnez **Oui** dans la zone de liste déroulante **Activation de la mise à disposition**.

Étape 3 Saisissez les paramètres.

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Rubriques connexes

Mises à jour de profil et mises à niveau du micrologiciel, à la page 37

Autoriser et configurer les mises à niveau du micrologiciel

Des mises à jour du micrologiciel peuvent être autorisées à intervalles réguliers. Le micrologiciel mis à jour est envoyé à partir d'un serveur sur le téléphone à l'aide de TFTP ou HTTP. La sécurité est moins un problème avec une mise à niveau du micrologiciel, car le micrologiciel ne contient pas d'informations personnelles.

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Sélectionnez **Voix** > **Mise à disposition**.

Étape 2 Dans la section **Mise à niveau de micrologiciel**, sélectionnez **Oui** dans la zone de liste déroulante **Activation de la mise à niveau**.

Étape 3 Saisissez les paramètres.

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Mise à niveau du micrologiciel par TFTP, HTTP ou HTTPS

Le téléphone prend en charge la mise à niveau d'une image unique par TFTP, HTTP, ou HTTPS.

Remarque Les régressions à des versions antérieures ne sont pas disponibles pour tous les périphériques. Pour plus d'informations, voir les notes de version de votre version du micrologiciel et du téléphone.

Avant de commencer

Le fichier de chargement du micrologiciel doit être téléchargé sur un serveur accessible.

Procédure

Étape 1 Renommer l'image en procédant comme suit :

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

où

`x8xx` est la série du téléphone, telle que 6841.

`aa-b-c` est le numéro de version, par exemple 10-4-1

Étape 2 Utilisez la commande **`tar -xzvf`** pour décompresser le composant tar.

Étape 3 Copiez le dossier dans un répertoire de téléchargement TFTP, HTTP, ou HTTPS

Étape 4 Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Étape 5 Sélectionnez **Voix -** > **Mise à disposition**.

Étape 6 Recherchez le nom de fichier de chargement qui se termine par **.loads** et l'ajouter à l'URL valide.

Étape 7 Cliquez sur **Envoyer toutes les modifications**.

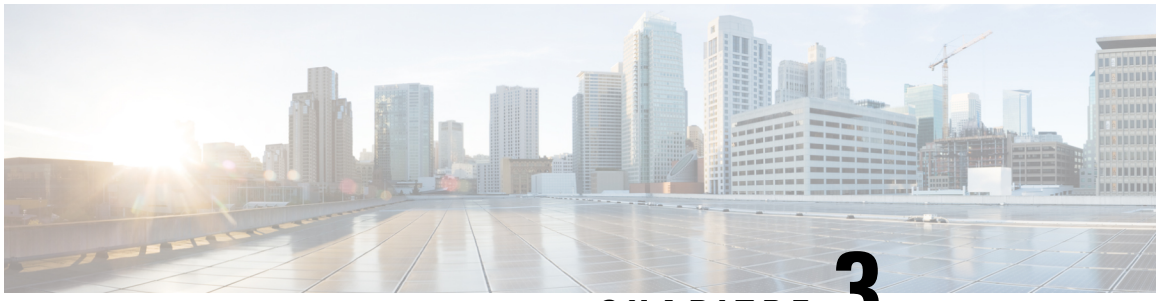
Mettre à niveau le micrologiciel à l'aide d'une commande de navigateur

Une commande de mise à niveau saisie dans la barre d'adresse de navigateur peut être utilisée pour mettre à niveau le micrologiciel sur un téléphone. Le téléphone ne se met à jour que lorsqu'il est inactif. La mise à jour est retentée automatiquement une fois l'appel terminé.

Procédure

Pour mettre à niveau le téléphone avec une URL dans un navigateur web, entrez la commande suivante :

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



CHAPITRE 3

Préprovisionnement interne et mise à disposition des serveurs

Préprovisionnement interne et mise à disposition des serveurs

Les fournisseurs de services préprovisionnent les téléphones, autres que les unités RC, grâce à un profil. Le profil de préprovisionnement peut comporter un ensemble restreint de paramètres qui resynchronisent le téléphone. Le profil peut comporter également une série complète des paramètres fournie par le serveur distant. Par défaut, le téléphone se resynchronise à la mise sous tension et à des intervalles qui sont configurés dans le profil. Lorsque l'utilisateur se connecte au téléphone dans les locaux du client, le périphérique télécharge le profil mie à jour et toute mise à jour du micrologiciel.

Ce processus de préprovisionnement, de déploiement et de mise à disposition à distance peut être réalisé de plusieurs manières.

Préparation du serveur et outils logiciels

Les exemples de ce chapitre requièrent la disponibilité d'un ou plusieurs serveurs. Ces serveurs peuvent être installés et exécutés sur un PC local :

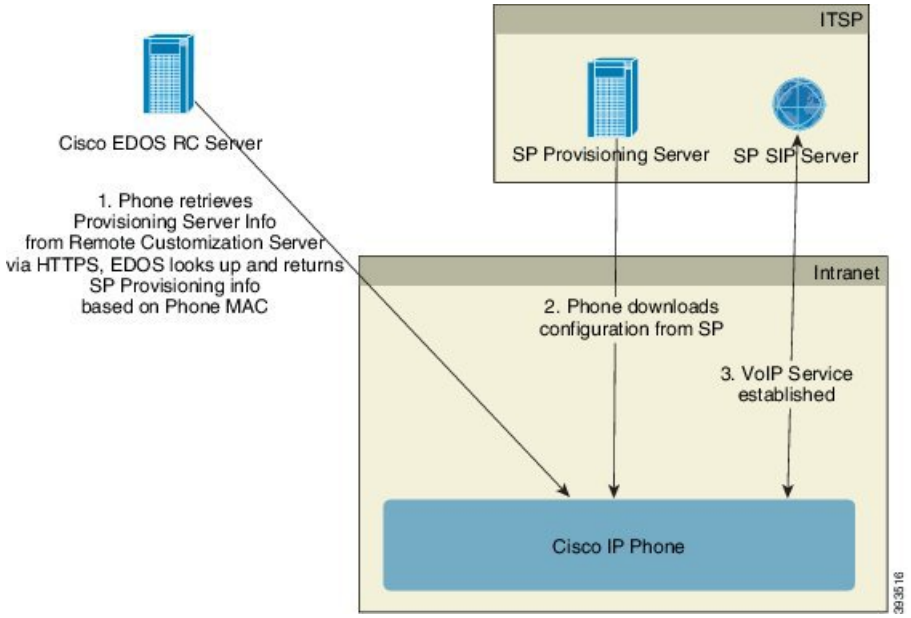
- TFTP (Port UDP 69)
- syslog (Port UDP 514)
- HTTP (TCP port 80)
- HTTPS (Port TCP 443).

Pour résoudre les problèmes de configuration du serveur, il est utile d'installer des clients pour chaque type de serveur sur une machine de serveur distincte. Cette pratique assure un fonctionnement correct du serveur, indépendamment de l'interaction avec les téléphones.

Nous vous recommandons également d'installer ces outils logiciels :

- Pour générer des profils de configuration, installez l'utilitaire de compression gzip open source.
- Pour le chiffrement de profil et les opérations HTTPS, installez le package de logiciels open source OpenSSL.
- Pour tester la génération de profil dynamique et la mise à disposition en une étape à distance à l'aide de HTTPS, nous vous recommandons un langage de script prenant en charge CGI. Les outils de langage Perl Open source constituent un exemple de ce langage de script.
- Pour vérifier les échanges sécurisés entre les serveurs de mise à disposition et les téléphones, installez un renifleur de paquet Ethernet (par exemple Ethereal/Wireshark, téléchargeable gratuitement). Capturez une trace des paquets Ethernet de l'interaction entre le téléphone et le serveur de mise à disposition. Pour ce faire, exécutez le renifleur de paquets sur un ordinateur connecté à un commutateur avec port miroir. Pour les transactions HTTPS, vous pouvez utiliser l'utilitaire ssldump.

Distribution de la personnalisation à distance (RC, Remote Customization)



Tous les téléphones contactent le serveur Cisco EDOS RC jusqu'à leur mise à disposition initiale.

Dans un modèle de distribution RC, un client achète un téléphone qui a déjà été associé à un fournisseur de services spécifique dans le serveur Cisco EDOS RC. Le fournisseur de Service de téléphonie Internet (ITSP) configure et gère un serveur de mise à disposition et enregistre les informations de serveur de mise à disposition sur le serveur Cisco EDOS RC.

Lorsque le téléphone est sous tension avec une connexion Internet, l'état de la personnalisation pour le téléphone non encore mis à disposition est **Ouvert**. Tout d'abord, le téléphone interroge le serveur local DHCP pour obtenir les informations sur e serveur de mise à disposition et définit l'état de la personnalisation du téléphone. Si la requête DHCP est réussie, l'état de la personnalisation est défini sur **Abandonné** et la RC n'est pas tentée car DHCP fournit les informations requises du serveur de mise à disposition.

Lorsqu'un téléphone se connecte à un réseau pour la première fois ou après une réinitialisation d'usine, s'il n'y a aucune configuration des options DHCP, il contacte un serveur d'activation du périphérique pour une mise à disposition sans contact. Les nouveaux téléphones utiliseront « activate.cisco.com » au lieu de «

webapps.cisco.com » pour la mise à disposition. Les téléphones dotés d'une version du micrologiciel antérieure à la 11.2(1), continueront à utiliser webapps.cisco.com. Cisco recommande que vous autorisiez les deux noms de domaine à franchir le pare-feu.

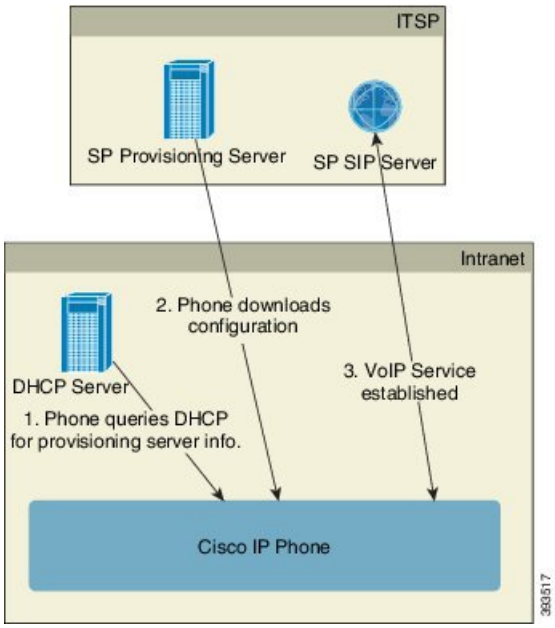
Si le serveur DHCP ne fournit pas d'informations sur le serveur mise à disposition, le téléphone interroge le serveur Cisco EDOS RC et fournit son adresse MAC et modèle, et définit l'état de la personnalisation sur **En attente**. Le serveur Cisco EDOS répond avec les informations du serveur de mise à disposition du fournisseur de services associé, y compris l'URL du serveur de mise à disposition, et l'état de personnalisation du téléphone est défini sur **En attente de personnalisation**. Le téléphone effectue ensuite une commande URL de resynchronisation pour récupérer la configuration du fournisseur de services et, en cas de réussite, l'état de la personnalisation est défini sur **Acquis**.

Si le serveur RC EDOS Cisco n'a pas un fournisseur de services associé au téléphone, l'état de la personnalisation du téléphone est défini sur **Indisponible**. Le téléphone peut être configuré manuellement ou une association du fournisseur de services du téléphone au serveur Cisco EDOS peut être ajoutée.

Si un téléphone est mis à disposition par l'intermédiaire de l'écran LCD ou de l'utilitaire de configuration web, avant que l'état de la personnalisation ne devienne **Acquis**, l'état de la personnalisation est défini sur **Abandonné** et le serveur EDOS Cisco ne sera pas interrogé, sauf si le téléphone est réinitialisé aux réglages d'usine.

Une fois que le téléphone a été mise à disposition, le serveur de RC EDOS Cisco n'est plus utilisé, sauf si le téléphone est réinitialisé aux réglages d'usine.

Préprovisionnement de périphérique interne



Avec la configuration par défaut d'usine Cisco, un téléphone tente automatiquement de se resynchroniser à un profil sur un serveur TFTP. Un serveur DHCP géré sur un réseau LAN fournit les informations sur le profil et le serveur TFTP qui est configuré pour préprovisionnement au périphérique. Le fournisseur de services connecte chaque nouveau téléphone au réseau local. Le téléphone se resynchronise automatiquement au serveur TFTP local et initialise son état interne dans la préparation du déploiement. Ce profil de préprovisionnement inclut généralement l'URL d'un serveur de mise à disposition à distance. Le serveur de

mise à disposition maintient le périphérique à jour une fois que ce dernier a été déployé et connecté au réseau du client.

Le code barres du périphérique préprovisionné peut être analysé pour enregistrer son adresse MAC ou son numéro de série avant que le téléphone ne soit livré au client. Ces informations peuvent servir à créer le profil auquel le téléphone se resynchronise.

Après avoir reçu le téléphone, le client doit le connecter à la liaison haut débit. Lors de la mise sous tension, le téléphone contacte le serveur de mise à disposition via l'URL configurée au moyen du préprovisionnement. Le téléphone peut donc se resynchroniser et mettre à jour le profil et le micrologiciel si nécessaire.

Rubriques connexes

Distribution de vente au détail, à la page 6
Mise à disposition TFTP, à la page 44

Configuration du serveur de mise à disposition

Cette section décrit la configuration requise pour la mise à disposition d'un téléphone à l'aide de plusieurs serveurs et de différents scénarios. Pour les besoins de ce document et pour les tests, les serveurs de mise à disposition sont installés et s'exécutent sur un PC local. En outre, des outils logiciels disponibles de manière courante sont utiles pour la mise à disposition des téléphones.

Mise à disposition TFTP

Les téléphones prennent en charge TFTP pour à la fois la resynchronisation de mise à disposition et les opérations de mise à niveau du micrologiciel. Lors du déploiement de périphériques à distance, HTTPS est recommandé, mais HTTP et TFTP peuvent également être utilisés. Ce processus exige alors le chiffrement des fichiers de mise à disposition pour accroître la sécurité, il offre une plus grande fiabilité, étant donné les mécanismes de protection NAT et du routeur. TFTP est utile pour les préprovisionnement internes d'un grand nombre de périphériques non encore mis à disposition.

Le téléphone est en mesure d'obtenir l'adresse IP d'un serveur TFTP directement à partir du serveur DHCP au moyen de l'option DHCP 66. Si un paramètre Profile_Rule est configuré avec le chemin d'accès de ce serveur TFTP, le périphérique télécharge son profil à partir du serveur TFTP. Le téléchargement se produit lorsque l'appareil est connecté à un réseau local et mis sous tension.

Le paramètre Profile_Rule fourni avec la configuration d'usine par défaut est *&PN*.cfg, où *&PN* représente le nom de modèle de téléphone.

Par exemple, pour un CP-6841-3PCC, le nom de fichier est CP-6841-3PCC.cfg.

Pour un périphérique comportant le profil par défaut d'usine, à la mise sous tension, le périphérique se resynchronise au fichier qui est spécifié par l'option DHCP 66 sur le serveur TFTP. Le chemin d'accès est relatif au répertoire racine virtuel du serveur TFTP.

Rubriques connexes

Préprovisionnement de périphérique interne, à la page 43

Contrôle de point de terminaison distant et NAT

Le téléphone est compatible avec la traduction d'adresses réseau (NAT) pour accéder à Internet au travers d'un routeur. Pour plus de sécurité, le routeur peut essayer de bloquer les paquets entrants non autorisés en mettant en œuvre la NAT symétrique, une stratégie de filtrage de paquets qui restreint de manière drastique

les paquets qui sont autorisés à entrer dans le réseau protégé à partir d'Internet. Pour cette raison, la mise à disposition à distance à l'aide de TFTP n'est pas recommandée.

VoIP peut coexister avec NAT uniquement lorsqu'une forme de traversée NAT est fournie. Configurer la Traversée simple de UDP par l'intermédiaire de NAT (STUN, Simple Traversal of UDP through NAT). Cette option nécessite que l'utilisateur dispose :

- d'une adresse IP (publique) externe dynamique à partir de votre service
- d'un ordinateur qui exécute un logiciel serveur STUN
- d'un périphérique de périmètre avec un mécanisme NAT asymétrique

Mise à disposition HTTP

Le téléphone se comporte comme un navigateur qui demande des pages web à un site Internet à distance. Cela fournit un moyen fiable d'atteindre le serveur de mise à disposition, même si un routeur client met en œuvre un NAT symétrique ou d'autres mécanismes de protection. HTTP et HTTPS fonctionnent de manière plus fiable que TFTP dans les déploiements à distance, en particulier lorsque les unités déployées sont connectées derrière des pare-feux résidentiels ou des routeurs NAT. HTTP et HTTPs sont utilisés indifféremment dans les descriptions de type de requête suivantes.

La mise à disposition de base fondée sur HTTP s'appuie sur la méthode HTTP GET pour récupérer des profils de configuration. En général, un fichier de configuration est créé pour chaque téléphone déployé, et ces fichiers sont enregistrés dans un répertoire de serveur HTTP. Lorsque le serveur reçoit la requête GET, il renvoie simplement le fichier qui est spécifié dans l'en-tête de la requête GET.

Au lieu d'un profil statique, le profil de configuration peut être généré dynamiquement en interrogeant une base de données client et en produisant le profil à la volée.

Lorsque le téléphone demande une resynchronisation, il peut utiliser la méthode HTTP POST pour demander les données de configuration de la resynchronisation. Le périphérique peut être configuré pour envoyer certaines informations d'identification et d'état sur le serveur dans le corps de la requête HTTP POST. Le serveur utilise ces informations pour générer le profil de configuration souhaité en réponse, ou pour stocker les informations d'état pour une analyse et un suivi ultérieurs.

Dans le cadre des demandes GET et POST, le téléphone inclut automatiquement des informations d'identification de base dans le champ Agent-utilisateur de l'en-tête de la demande. Ces informations comportent le fabricant, le nom du produit, la version actuelle du micrologiciel et le numéro de série du périphérique.

L'exemple suivant est le champ de demande Agent-utilisateur d'un CP-6841-3PCC :

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

Lorsque le téléphone est configuré pour se resynchroniser à un profil de configuration en utilisant le protocole HTTP, il est recommandé d'utiliser HTTPS ou que le profil soit chiffré pour assurer la protection des informations confidentielles. Les profils chiffrés que le téléphone télécharge en utilisant le protocole HTTP évitent le risque d'exposition des informations confidentielles contenues dans le profil de configuration. Ce mode de resynchronisation génère une charge de calcul inférieure sur le serveur de mise à disposition par rapport à l'utilisation de HTTPS.

Le téléphone peut déchiffrer des profils chiffrés avec l'une de ces méthodes de chiffrement :

- Chiffrement AES-256-CBC

- Chiffrement basé sur RFC-8188 avec chiffrement AES-128-GCM

Remarque Les téléphones prennent en charge HTTP Version 1.0, HTTP Version 1.1 et le codage de bloc lorsque HTTP Version 1.1 est le protocole de transport négociés.

Gestion du code d'état HTTP lors de la resynchronisation et de la mise à niveau

Le téléphone prend en charge la réponse HTTP de mise à disposition à distance (resynchronisation). Le comportement du téléphone actuel est classé de trois manières différentes :

- A : succès, où les valeurs « Resync Periodic » et « Resync Random Delay » déterminent les demandes suivantes.
- B : échec lorsque le fichier est introuvable ou le profil est endommagé. La valeur « Resync Error Retry Delay » détermine les demandes suivantes.
- C : autre panne lorsqu'une URL ou adresse IP erronée entraîne une erreur de connexion. La valeur « Resync Error Retry Delay » détermine les demandes suivantes.

Tableau 2 : Comportement du téléphone pour les réponses HTTP

Code d'état HTTP	Description	Comportement du téléphone
301 Déplacé définitivement	La requête présente et les requêtes futures doivent être dirigées vers un nouvel emplacement.	Réessayez le requête immédiatement avec le nouvel emplacement.
302 Trouvé	Connu comme déplacé temporairement.	Réessayez le requête immédiatement avec le nouvel emplacement.
3xx	Autres réponses 3xx non traitées.	C
400 Demande incorrecte	Impossible de répondre à la demande en raison d'une syntaxe incorrecte.	C
401 Non autorisé	Défaut d'authentification d'accès de base ou résumé.	Réessayez immédiatement la demande avec les informations d'authentification. Nombre maximal de 2 tentatives. En cas de panne, le comportement du téléphone est C.
403 Interdit	Le serveur refuse de répondre.	C
404 Introuvable	Ressource demandée introuvable. Les demandes suivantes du client sont autorisées.	B

Code d'état HTTP	Description	Comportement du téléphone
407 Authentification du proxy requise	Défaut d'authentification d'accès de base ou résumé.	Réessayez immédiatement la demande avec les informations d'authentification. Nombre maximal de deux tentatives. En cas de panne, le comportement du téléphone est C.
4xx	Les autres codes d'état d'erreur client ne sont pas traités.	C
500 erreur de serveur interne	Message d'erreur générique.	Le comportement du téléphone est de type C
501 Non mis en œuvre	Le serveur ne reconnaît pas la méthode de la demande, ou ne dispose pas de la possibilité de répondre à la demande.	Le comportement du téléphone est de type C
502 Passerelle incorrecte	Le serveur agit en tant que passerelle ou proxy et reçoit une réponse non valide à partir du serveur en amont.	Le comportement du téléphone est de type C
503 Service non disponible	Le serveur n'est actuellement pas disponible (surchargé ou à l'arrêt pour maintenance). Il s'agit d'un état temporaire.	Le comportement du téléphone est de type C
504 Expiration de la passerelle	Le serveur agit en tant que passerelle ou proxy et ne reçoit pas de réponse en temps opportun du serveur en amont.	C
5xx	Autre erreur du serveur	C

Mise à disposition HTTPS

Pour accroître la sécurité de gestion des unités déployées à distance, le téléphone prend en charge le protocole HTTPS pour la mise à disposition. Chaque téléphone exécute un certificat client SSL unique (et sa clé privée associée), en plus d'un certificat racine du serveur d'autorité de certification Sipura. Ce dernier permet au téléphone de reconnaître les serveurs de mise à disposition autorisés et de rejeter les serveurs non autorisés. Par ailleurs, le certificat client permet au serveur de mise à disposition d'identifier le périphérique qui émet la demande.

Dans le cas d'un fournisseur de services gérant le déploiement à l'aide de HTTPS, un certificat de serveur doit être généré pour chaque serveur de mise à disposition auquel un téléphone se resynchronise à l'aide de HTTPS. Le certificat du serveur doit être signé par la clé racine de l'autorité de certification du serveur Cisco, dont le certificat est utilisé par toutes les unités déployées. Pour obtenir un certificat de serveur signé, le fournisseur de services doit renvoyer une demande de signature de certificat à Cisco, qui signe le certificat du serveur et le renvoie pour installation sur le serveur de mise à disposition.

Le certificat du serveur de mise à disposition doit contenir le champ nom commun (CN) et le nom de domaine complet (FQDN) de l'hôte du serveur en cours d'exécution dans l'objet. Il peut contenir éventuellement des informations à la suite du FQDN de l'hôte, séparées par une barre oblique (/). Les exemples suivants sont des entrées CN acceptées comme valides par le téléphone :

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

Outre la possibilité de vérifier le certificat du serveur, le téléphone teste l'adresse IP du serveur par rapport à une recherche DNS du nom du serveur spécifié dans le certificat du serveur.

Obtenir un certificat de serveur signé

L'utilitaire OpenSSL peut générer un demande de signature de certificat. L'exemple suivant illustre la commande **openssl** qui génère une paire de clés publique/privée 1024 bits RSA et une demande de signature de certificat :

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

Cette commande génère la clé privée du serveur dans **privkey.pem** et la demande de signature de certificat correspondante dans **provserver.csr** . Le fournisseur de services conserve de manière sécurisée **privkey.pem**, et envoie **provserver.csr** à Cisco pour signature. Dès réception du fichier **provserver.csr**, Cisco génère **provserver.crt**, le certificat du serveur signé.

Procédure

Étape 1 Accédez à https://software.cisco.com/software/cda/home et connectez-vous à l'aide de vos informations d'identification CCO.

Remarque Lorsqu'un téléphone se connecte à un réseau pour la première fois ou après une réinitialisation d'usine, et qu'il n'y a aucune configuration des options DHCP, il contacte un serveur d'activation du périphérique pour une mise à disposition sans contact. Les nouveaux téléphones utilisent « activate.cisco.com » au lieu de « webapps.cisco.com » pour la mise à disposition. Les téléphones dotés d'une version du micrologiciel antérieure à la 11.2(1), continuent à utiliser « webapps.cisco.com. » Nous recommandons que vous autorisiez les deux noms de domaine à franchir le pare-feu.

Étape 2 Sélectionnez **Gestion des certificats**.

Sur l'onglet **Signature du CSR**, le CSR de l'étape précédente est chargé pour signature.

Étape 3 À partir de la zone de liste déroulante **Sélectionner un produit**, sélectionnez **SPA1xx micrologiciel 1.3.3 et version ultérieure / SPA232D micrologiciel 1.3.3 et version ultérieure / SPA5xx micrologiciel 7.5.6 et version ultérieure / CP-78xx-3PCC/CP-88xx-3PCC**.

Remarque Ce produit inclut les téléphones multiplateformes IP Cisco 6800.

Étape 4 Dans le champ **Fichier CSR**, cliquez sur **Parcourir** et sélectionnez le CSR pour signature.

Étape 5 Sélectionnez la méthode de cryptage :

- MD5
- SHA1
- SHA256

Cisco recommande que vous sélectionniez le cryptage SHA256.

Étape 6 À partir de la zone de liste déroulante **Durée de la connexion**, sélectionnez la durée qui s'applique (par exemple, un an).

Étape 7 Cliquez sur **Signer la demande de certificat** .

Étape 8 Sélectionnez l'une des options suivantes pour recevoir le certificat signé :

- **Saisir l'adresse de courrier électronique du destinataire** : si vous souhaitez recevoir le certificat par courrier électronique, entrez votre adresse électronique dans ce champ.
- **Téléchargement** : si vous souhaitez télécharger le certificat signé, sélectionnez cette option.

Étape 9 Cliquez sur **Soumettre**.

Le certificat du serveur signé est alors soit envoyé par e-mail à l'adresse de courrier électronique précédemment fournie ou téléchargé.

Certificat racine du client d'autorité de certification de téléphone multiplateforme

Cisco fournit également un certificat racine client d'autorité de certification de téléphone multiplateforme au fournisseur de services. Ce certificat racine certifie l'authenticité du certificat client que chaque téléphone transporte. Les téléphones multiplateformes prennent également en charge les certificats signés par des tiers tels que ceux fournis par Verisign, Cybertrust et autres.

Le certificat client unique que propose chaque périphérique lors d'une session HTTPS comporte des informations d'identification qui sont intégrées dans le champ objet. Ces informations peuvent être rendues disponibles par le serveur HTTPS à un script CGI appelé pour traiter les demandes sécurisées. En particulier, l'objet du certificat indique le nom de produit de l'unité (élément OU), l'adresse MAC (élément S) et le numéro de série (élément L).

L'exemple suivant tiré du téléphone IP Cisco 6841 multiplateforme de champ de sujet de certificat client affiche les éléments suivants :

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

Pour déterminer si un téléphone comporte un certificat individuel, utilisez la variable macro $CCERT de mise à disposition. La valeur de la variable est étendue en installé ou Non installé, en fonction de la présence ou l'absence d'un certificat client unique. Dans le cas d'un certificat générique, il est possible d'obtenir le numéro de série de l'unité à partir de l'en-tête de demande HTTP dans le champ Agent utilisateur.

Les serveurs HTTPS peuvent être configurés pour demander les certificats SSL des clients en cours de connexion. S'il est activé, le serveur peut utiliser le certificat racine client d'autorité de certification de téléphone multiplateforme que Cisco fournit pour vérifier le certificat du client. Le serveur peut ensuite fournir les informations de certificat à un script CGI pour traitement.

L'emplacement de stockage des certificats peut varier. Par exemple, dans une installation Apache, les chemins d'accès aux fichiers pour le stockage du certificat signé par le serveur de mise à disposition, de sa clé privée associée et du certificat racine client de l'autorité de certification de téléphone multiplateforme sont les suivants :

```
# 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
```

Pour plus d'informations, reportez-vous à la documentation relative à un serveur HTTPS.

L'autorité de certification racine de client Cisco signe chaque certificat unique. Le certificat racine correspondant est proposé aux prestataires de services en vue de l'authentification client.

Serveurs redondants de mise à disposition

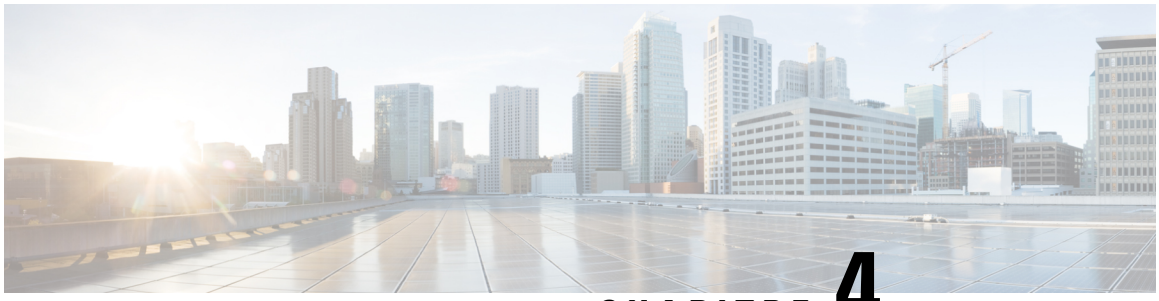
Le serveur de mise à disposition peut être précisé avec une adresse IP ou avec un Nom de Domaine Complet (FQDN). L'utilisation d'un nom de domaine complet facilite le déploiement de serveurs redondants de mise à disposition. Lorsque le serveur de mise à disposition est identifié à travers un nom de domaine complet, le téléphone tente de résoudre le nom de domaine complet vers une adresse IP à travers le DNS. Seuls les enregistrements A DNS sont pris en charge pour la mise à disposition ; la résolution d'adresses DNS SRV n'est pas disponible pour la mise à disposition. Le téléphone continue de traiter les enregistrements A jusqu'à ce qu'un serveur réponde. Si aucun serveur associé aux enregistrements A ne répond, le téléphone enregistre une erreur sur le serveur syslog.

Serveur Syslog

Si un serveur syslog est configuré sur le téléphone grâce à l'utilisation des paramètres <serveur Syslog>, les opérations de mise à niveau et de resynchronisation envoient des messages au serveur syslog. Un message peut être généré au début d'une demande de fichier distant (chargement de micrologiciel ou profil de configuration) et à la fin de l'opération (indiquant la réussite ou échec).

Les messages enregistrés sont configurés dans les paramètres suivants et font l'objet d'expansion de macro dans les messages syslog réels :

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg



CHAPITRE 4

Exemples de mise à disposition

Vue d'ensemble des exemples de mise à disposition

Ce chapitre fournit des exemples de procédures pour transférer les profils de configuration entre le téléphone et le serveur de mise à disposition.

Pour plus d'informations sur la création des profils de configuration, reportez-vous à Formats de mise à disposition, à la page 15.

Resynchronisation de base

Cette section décrit les fonctionnalités de base de resynchronisation des téléphones.

Resynchronisation TFTP

Le téléphone prend en charge plusieurs protocoles réseau pour récupérer des profils de configuration. Le protocole de transfert de profil le plus élémentaire est TFTP (RFC1350). TFTP est largement utilisé pour la mise à disposition des périphériques réseau dans les réseaux privés. Bien que non recommandé pour le déploiement de points d'extrémité à distance sur Internet, TFTP peut être pratique pour le déploiement dans de petites entreprises, le préprovisionnement interne et le développement et les tests. Reportez-vous à Préprovisionnement de périphérique interne, à la page 43 pour plus d'informations sur le préprovisionnement en interne. Dans la procédure suivante, un profil est modifié après avoir téléchargé un fichier à partir d'un serveur TFTP.

Procédure

Étape 1 Dans un environnement de réseau local, branchez un ordinateur et un téléphone à un concentrateur, à un commutateur ou à un petit routeur.

Étape 2 Sur le PC, installez et activez un serveur TFTP.

Étape 3 Utilisez un éditeur de texte pour créer un profil de configuration qui définit la valeur de GPP_A à 12345678, comme illustré dans l'exemple.

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

Étape 4 Enregistrez le profil avec le nom `basic.txt` dans le répertoire racine du serveur TFTP.

Vous pouvez vérifier que le serveur TFTP est correctement configuré : demandez le fichier `basic.txt` à l'aide d'un client TFTP autre que le téléphone. Si possible, utilisez un client TFTP qui est en cours d'exécution sur un hôte distinct du serveur de mise à disposition.

Étape 5 Ouvrez le navigateur web PC à la page configuration avancée/d'administration. Par exemple, si l'adresse IP du téléphone est 192.168.1.100 :

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

Étape 6 Sélectionnez l'onglet **Voix** > **Mise à disposition** et vérifiez les valeurs des paramètres généraux GPP_A à GPP_P. Ceux-ci devraient être vides.

Étape 7 Resynchronisez le téléphone de test sur le profil de configuration `basic.txt` en ouvrant l'URL de resynchronisation dans une fenêtre de navigateur web.

Si l'adresse IP du serveur TFTP est 192.168.1.200, la commande doit être semblable à l'exemple suivant :

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

Lorsque le téléphone reçoit cette commande, le périphérique à l'adresse 192.168.1.100 demande le fichier `basic.txt` au serveur TFTP à l'adresse IP 192.168.1.200. Le téléphone traite alors le fichier téléchargé et met à jour le paramètre GPP_A avec la valeur 12345678.

Étape 8 Vérifiez que le paramètre a été correctement mise à jour : actualisez la page de configuration dans le navigateur web du PC, puis sélectionnez l'onglet **Voix** > **Mie à disposition**.

Le paramètre GPP_A doit maintenant contenir la valeur 12345678.

Utilisez Syslog pour journaliser les messages

Le téléphone envoie un message syslog au serveur syslog désigné lorsque le périphérique est sur le point d'effectuer une resynchronisation à un serveur de mise à disposition et une fois la resynchronisation terminée ou en échec. Pour identifier ce serveur, vous pouvez accéder à la page web administration du téléphone (voir Accéder à la page web du téléphone, à la page 9), sélectionnez **Voix** > **Système** et identifier le serveur grâce au paramètre **Serveur Syslog** de la section **Configuration réseau facultative**. Configurez l'adresse IP du serveur syslog sur le périphérique et observez les messages qui sont générés pendant les procédures restantes.

Procédure

Étape 1 Sur le PC, installez et activez un serveur syslog.

Étape 2 Programmez l'adresse IP de l'ordinateur dans le paramètre serveur Syslog_Server du profil et envoyez la modification :

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

Étape 3 Cliquez sur l'onglet **Système** et saisissez la valeur de votre serveur syslog local dans le paramètre Syslog_Server.

Étape 4 Répétez l'opération de resynchronisation comme indiqué en Resynchronisation TFTP, à la page 51.

Le périphérique génère deux messages syslog au cours de la resynchronisation. Le premier message indique qu'une demande est en cours. Le deuxième message marque la réussite ou l'échec de la resynchronisation.

Étape 5 Vérifiez que votre serveur syslog a reçu des messages similaires aux messages suivants :

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

Des messages détaillés sont disponibles en programmant un paramètre Debug_Server (au lieu du paramètre Syslog_Server) associé à l'adresse IP du serveur syslog et en définissant le Debug_Level à une valeur comprise entre 0 et 3 (3 est la plus détaillée) :

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

Le contenu de ces messages peut être configuré en utilisant les paramètres suivants :

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Si les paramètres suivants sont effacés, le message syslog correspondant n'est pas généré.

Resynchroniser un périphérique automatiquement

Un périphérique peut périodiquement se resynchroniser au serveur de mise à disposition pour s'assurer que les modifications de profil sur le serveur sont répercutées sur le périphérique de point de terminaison (par opposition à envoyer une demande de resynchronisation explicite au point de terminaison).

Pour faire en sorte que le téléphone se resynchronise périodiquement à un serveur, une URL de profil de configuration est définie à l'aide du paramètre Profile_Rule, et une période de resynchronisation est définie à l'aide du paramètre Resync_Periodic.

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Sélectionnez **Voix -** > **Mise à disposition**.

Étape 2 Définissez le paramètre Profile_Rule de règle de profil. Cet exemple suppose que l'adresse IP du serveur TFTP est 192.168.1.200.

Étape 3 Saisissez dans le champ **Resync Periodic**, une valeur faible pour les tests, telle que **30** secondes.

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Avec les nouveaux paramètres, le téléphone se resynchronise deux fois par minute au fichier de configuration que spécifie l'URL.

Étape 5 Observez les messages de résultats de la trace syslog (comme indiqué à la section Utilisez Syslog pour journaliser les messages, à la page 52).

Étape 6 Vérifiez que le champ **Resync On Reset** est défini sur **Oui**.

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

Étape 7 Éteignez et rallumez le téléphone pour forcer la resynchronisation au serveur de mise à disposition.

Si l'opération de resynchronisation échoue pour une raison quelconque, telle que l'absence de réponse du serveur, l'unité attend (pour le nombre de secondes configuré dans **Resync Error Retry Delay**) avant de tenter à nouveau la resynchronisation. Si **Resync_Error_Retry_Delay** est défini sur 0, le téléphone ne tente pas d'effectuer à nouveau une resynchronisation après une tentative de resynchronisation infructueuse.

Étape 8 (Facultatif) Définissez la valeur du champ **Resync Error Retry Delay** à une valeur faible, telle que **30**.

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

Étape 9 Désactivez le serveur TFTP et examinez les résultats dans la sortie syslog.

Profils uniques, expansion de macro et HTTP

Dans un déploiement dans lequel chaque téléphone doit être configuré avec des valeurs distinctes pour certains paramètres, par exemple User_ID ou Display_Name, le fournisseur de services peut créer un profil unique pour chaque périphérique déployé et héberger ces profils sur un serveur de mise à disposition. Chaque téléphone, à son tour, doit être configuré pour se resynchroniser à son propre profil selon une convention de nommage de profil prédéterminée.

La syntaxe de l'URL de profil peut comporter des informations d'identification qui sont spécifiques à chaque téléphone, telles que l'adresse MAC ou le numéro de série, à l'aide de l'expansion de macro des variables intégrées. L'expansion de macro élimine la nécessité de spécifier ces valeurs à plusieurs emplacements au sein de chaque profil.

Une règle de profil subit une expansion de macro avant que la règle ne soit appliquée au téléphone. L'expansion de macro contrôle un nombre de valeurs, par exemple :

- $MA affiche de manière étendue l'adresse MAC de l'unité sur 12 chiffres (à l'aide de chiffres hexadécimaux en minuscules). Par exemple, 000e08abcdef.

- $SN affiche le numéro de série de l'unité. Par exemple, 88012BA01234.

D'autres valeurs peuvent faire l'objet d'expansion de macro de cette manière, y compris tous les paramètres généraux GPP_A à GPP_P. Un exemple de ce processus est visible en Resynchronisation TFTP, à la page 51. L'expansion de macro n'est pas limitée au nom de fichier URL, mais peut également être appliquée à toute partie du paramètre de règle de profil. Ces paramètres sont référencées de $A à $P. Pour obtenir la liste complète des variables qui sont disponibles pour l'expansion de macro, reportez-vous à Variables d'expansion de macro, à la page 79.

Dans cet exercice, un profil spécifique à un téléphone est mis à disposition sur un serveur TFTP.

Exercice : Mettez à disposition un profil de téléphone IP spécifique sur un serveur TFTP

Procédure

Étape 1 Obtenez l'adresse MAC du téléphone à partir de son étiquette du produit. (L'adresse MAC est le numéro, constitué de chiffres et de caractères hexadécimaux en minuscules, par exemple 000e08aabbcc.

Étape 2 Copiez le fichier de configuration `basic.txt` (décrit à la section Resynchronisation TFTP, à la page 51) dans un nouveau fichier nommé `CP-xxxx-3PCC macaddress.cfg` (en remplaçant `xxxx` par le numéro de modèle et `macaddress` par l'adresse MAC du téléphone).

Étape 3 Déplacez le nouveau fichier dans le répertoire racine virtuel du serveur TFTP.

Étape 4 Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Étape 5 Sélectionnez **Voix -** > **Mise à disposition**.

Étape 6 Saisissez `tftp://192.168.1.200/CP-6841-3PCC $MA.cfg` dans le champ **Règle de profil**.

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

Étape 7 Cliquez sur **Envoyer toutes les modifications**. Cela entraîne un redémarrage et une resynchronisation immédiats.

Lorsque la resynchronisation suivante se produit, le téléphone récupère le nouveau fichier en développant l'expression macro $MA en son adresse MAC.

HTTP GET Resync (Resynchronisation HTTP GET)

HTTP fournit un mécanisme de resynchronisation plus fiable que TFTP car HTTP établit une connexion TCP et TFTP utilise le protocole UDP moins fiable. En outre, les serveurs HTTP offrent un meilleur filtrage et fonctions de journalisation par rapport aux serveurs TFTP.

Côté client, le téléphone ne nécessite pas de paramètre de configuration spécial sur le serveur pour être en mesure de se resynchroniser en utilisant le protocole HTTP. La syntaxe du paramètre Profile_Rule pour l'utilisation de HTTP avec la méthode GET est similaire à la syntaxe utilisée pour TFTP. Si un navigateur web standard peut récupérer un profil à partir de votre serveur HTTP, le téléphone doit être en mesure de le faire également.

Exercice : resynchronisation HTTP GET

Procédure

Étape 1 Installez un serveur HTTP sur l'ordinateur local ou un autre hôte accessible.

Le serveur Apache open source peut être téléchargé à partir d'Internet.

Étape 2 Copiez le profil de configuration `basic.txt` (décrit en Resynchronisation TFTP, à la page 51) sur le répertoire racine virtuel du serveur installé.

Étape 3 Pour vérifier que l'installation de serveur est adéquate et l'accès au fichier `basic.txt`, accédez au profil à l'aide d'un navigateur web.

Étape 4 Modifiez le paramètre Profile_Rule du téléphone de test pour pointer vers le serveur HTTP à la place du serveur TFTP, afin de télécharger son profil périodiquement.

Par exemple, en supposant que le serveur HTTP est à l'adresse 192.168.1.300, saisissez la valeur suivante :

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

Étape 5 Cliquez sur **Envoyer toutes les modifications**. Cela entraîne un redémarrage et une resynchronisation immédiats.

Étape 6 Observez les messages syslog que le téléphone envoie. Les resynchronisations périodiques doivent maintenant obtenir le profil à partir du serveur HTTP.

Étape 7 Dans les journaux du serveur HTTP, observez comment les informations qui identifient le téléphone de test apparaissent dans le journal des agents de l'utilisateur.

Ces informations doivent inclure le fabricant, le nom du produit, la version actuelle du micrologiciel et le numéro de série.

Mise à disposition au moyen de Cisco XML

Pour chacun des téléphones, désignés en tant que xxxx ici, vous pouvez configurer via les fonctions Cisco XML.

Vous pouvez envoyer un objet XML au téléphone par un paquet SIP Notify ou un HTTP Post à l'interface CGI du téléphone : `http://IPAddressPhone/CGI/Execute`.

Le CP-xxxx-3PCC étend la fonctionnalité Cisco XML pour prendre en charge la mise à disposition au moyen d'un objet XML :

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

Après avoir reçu l'objet XML, le téléphone télécharge le fichier de mise à disposition à partir de [profile-rule]. Cette règle utilise des macros pour simplifier le développement de l'application de services XML.

Résolution d'URL avec une expansion de macro

Les sous-répertoires avec plusieurs profils sur le serveur fournissent une méthode pratique pour gérer un grand nombre de périphériques déployés. L'URL de profil peut contenir :

- Un nom de serveur de mise à disposition ou une adresse IP explicite. Si le profil identifie le serveur de mise à disposition par son nom, le téléphone effectue une recherche DNS pour résoudre le nom.
- Un port de serveur non standard est spécifié dans l'URL à l'aide de la syntaxe standard `:port` suivant le nom du serveur.
- Le sous-répertoire du répertoire racine virtuel du serveur où le profil est stocké, spécifié à l'aide de la notation URL standard et géré par expansion de macro.

Par exemple, le paramètre Profile_Rule suivant demande le profil ($PN.cfg), dans le sous-répertoire du serveur `/cisco/config`, à partir du serveur TFTP qui est en cours d'exécution sur l'hôte prov.telco.com état à l'écoute d'une connexion sur le port 6900 :

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

Un profil pour chaque téléphone, peut être identifié dans les paramètres généraux, dont la valeur est référencée dans une règle de profil commune à l'aide de l'expansion de macro.

Par exemple, supposons que GPP_B soit défini en tant que `Dj6Lmp23Q`.

Le paramètre Profile_Rule a la valeur :

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

Lorsque le périphérique se resynchronise et que les macros sont développées, le téléphone comportant l'adresse MAC 000e08012345 demande le profil portant le nom qui contient l'adresse MAC du périphérique à l'URL suivante :

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

Protocole HTTPS sécurisé de resynchronisation

Ces mécanismes sont disponibles sur le téléphone pour effectuer une synchronisation utilisant un processus de communication sécurisée :

- Resynchronisation HTTPS de base
- HTTPS avec authentification par certificat client
- Filtrage client HTTPS et contenu dynamique

Resynchronisation HTTPS de base

HTTPS ajoute SSL à HTTP pour mise à disposition à distance afin que le :

- Le téléphone puisse authentifier le serveur de mise à disposition.
- Le serveur de mise à disposition puisse authentifier le téléphone.
- la confidentialité des informations échangées entre le téléphone et le serveur de mise à disposition soit assurée.

SSL génère et échange des clés secrètes (symétriques) pour chaque connexion entre le téléphone et le serveur à l'aide des paires de clés publique/privée préinstallées dans le téléphone et le serveur de configuration.

Côté client, le téléphone ne nécessite pas de paramètre de configuration spécial sur le serveur pour être en mesure de se resynchroniser en utilisant le protocole HTTPS. La syntaxe du paramètre Profile_Rule pour l'utilisation de HTTPS avec la méthode GET est similaire à la syntaxe utilisée pour HTTP ou TFTP. Si un navigateur web standard peut récupérer un profil à partir de votre serveur HTTPS, le téléphone doit être en mesure de le faire également.

En plus de l'installation d'un serveur HTTPS, un certificat de serveur SSL signé par Cisco doit être installé sur le serveur de configuration. Les périphériques ne peuvent pas se resynchroniser à un serveur qui utilise HTTPS, sauf si le serveur fournit un certificat de serveur signé par Cisco. Des instructions pour la création des certificats SSL signés pour les produits vocaux peuvent être consultées sur https://supportforums.cisco.com/docs/DOC-9852.

Exercice : resynchronisation HTTPS de base

Procédure

Étape 1 Installez un serveur HTTPS sur un hôte dont l'adresse IP est connue du serveur DNS de réseau via la traduction du nom d'hôte normale.

Le serveur Apache open source peut être configuré pour fonctionner comme un serveur HTTPS s'il est installé avec le package mod_ssl open source.

Étape 2 Générez une demande de signature de certificat de serveur pour le serveur. Pour cette étape, vous devrez peut-être installer le package OpenSSL open source ou un logiciel équivalent. Si vous utilisez OpenSSL, la commande pour générer le fichier de base CSR est la suivante :

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

Cette commande génère une paire de clés publique/privée, qui est enregistrée dans le fichier `privkey.pem`.

Étape 3 Envoyez le fichier CSR (provserver.csr) à Cisco pour signature.

Un certificat signé de serveur est renvoyé (provserver.cert) ainsi qu'un certificat racine du client d'autorité de certification Sipura, spacroot.cert.

Pour plus d'informations, reportez-vous à la section https://supportforums.cisco.com/docs/DOC-9852.

Étape 4 Stockez le certificat du serveur signé, le fichier de paire de clés privées et le certificat racine du client dans les emplacements appropriés sur le serveur.

Dans le cas d'une installation Apache sur Linux, ces emplacements sont généralement les suivants :

```
# 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
```

Étape 5 Redémarrez le serveur.

Étape 6 Copiez le fichier de configuration `basic.txt` (décrit en Resynchronisation TFTP, à la page 51) sur le répertoire racine virtuel du serveur HTTPS installé.

Étape 7 Vérifiez que le serveur fonctionne correctement en téléchargeant `basic.txt` à partir du serveur HTTPS à l'aide d'un navigateur standard depuis l'ordinateur local.

Étape 8 Vérifiez le certificat de serveur fourni par le serveur.

Le navigateur ne reconnaît sans doute pas le certificat comme étant valide, sauf si le navigateur a été préconfiguré pour accepter Cisco comme une autorité de certification racine. Toutefois, les téléphones s'attendent à ce que le certificat soit signé de cette façon.

Modifiez le paramètre Profile_Rule du périphérique de test pour qu'il contienne une référence au serveur HTTPS, par exemple :

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

Cet exemple suppose que le nom du serveur HTTPS est **`my.server.com`**.

Étape 9 Cliquez sur **Envoyer toutes les modifications**.

Étape 10 Observez la trace syslog que le téléphone envoie.

Le message syslog doit indiquer que la resynchronisation a extrait le profil du serveur HTTPS.

Étape 11 (facultatif) (Facultatif) Utilisez un analyseur de protocole Ethernet sur le sous-réseau du téléphone pour vérifier que les paquets sont chiffrés.

Dans cet exercice, la vérification du certificat client n'est pas activée. La connexion entre le téléphone et le serveur est chiffrée. Toutefois, le transfert n'est pas sécurisé, car n'importe quel client peut se connecter au serveur et demander le fichier, en fonction des connaissances du nom de fichier et de l'emplacement du répertoire. Pour une resynchronisation sécurisée, le serveur doit également authentifier le client, comme indiqué dans l'exercice décrit en HTTPS avec authentification par certificat client, à la page 59.

HTTPS avec authentification par certificat client

Dans la configuration usine par défaut, le serveur ne demande pas de certificat client SSL à un client. Le transfert du profil n'est pas sécurisé, car tous les clients peuvent se connecter au serveur et demander le profil. Vous pouvez modifier la configuration pour activer l'authentification client ; le serveur requiert un certificat client pour authentifier le téléphone avant d'accepter une demande de connexion.

En raison de cette condition, l'opération de resynchronisation ne peut pas être testée indépendamment à l'aide d'un navigateur qui ne contient pas les informations d'identification correctes. L'échange de clés SSL au sein de la connexion HTTPS entre le téléphone de test et le serveur peut être observé grâce à l'utilitaire ssldump. La trace de l'utilitaire montre l'interaction entre le client et serveur.

Exercice : HTTPS avec authentification par certificat client

Procédure

Étape 1 Activez l'authentification par certificat client sur le serveur HTTPS.

Étape 2 Dans Apache (v.2), définissez les éléments suivants dans le fichier de configuration du serveur :

```
SSLVerifyClient  require
```

Vérifiez également que le spacroot.cert a été enregistré comme illustré dans l'exercice Resynchronisation HTTPS de base, à la page 57.

Étape 3 Redémarrez le serveur HTTPS et observez la trace syslog à partir du téléphone.

Chaque resynchronisation avec le serveur effectue désormais l'authentification symétrique, afin que le certificat du serveur et le certificat client soient vérifiés avant que le profil ne soit transféré.

Étape 4 Ssldump permet de capturer une connexion de resynchronisation entre le téléphone et le serveur HTTPS.

Si la vérification du certificat client est correctement activée sur le serveur, la trace ssldump montre l'échange symétrique des certificats (tout d'abord du serveur au client, puis du client au serveur) avant l'échange des paquets chiffrés que contient le profil.

Avec l'authentification client activée, seul un téléphone avec une adresse MAC qui correspond à un certificat client valide peut demander le profil à partir du serveur de mise à disposition. Le serveur rejette une demande effectuée à partir d'un navigateur ordinaire ou de tout autre périphérique non autorisé.

Filtrage client HTTPS et contenu dynamique

Si le serveur HTTPS est configuré pour demander un certificat client, les informations contenues dans le certificat identifient le téléphone qui se resynchronise et fournissent cette information avec les informations de configuration appropriées.

Le serveur HTTPS rend disponible les informations de certificat pour les scripts CGI (ou les programmes CGI compilés) qui sont appelés dans le cadre de la demande de resynchronisation. Dans un but d'illustration, cet exercice utilise le langage de script Perl open source et suppose qu'Apache (v.2) est utilisé comme serveur HTTPS.

Procédure

Étape 1 Installez Perl sur l'hôte où le serveur HTTPS est en cours d'exécution.

Étape 2 Générez le script de Perl reflector suivant :

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

Étape 3 Enregistrez ce fichier avec le nom de fichier `reflect.pl`, avec l'autorisation exécutable (chmod 755 sur Linux), dans le répertoire de scripts CGI du serveur HTTPS.

Étape 4 Vérifiez l'accessibilité des scripts CGI sur le serveur (c'est-à-dire, `/cgi-bin/...`).

Étape 5 Modifiez le paramètre Profile_Rule sur le périphérique de test pour une resynchronisation au script reflector, comme dans l'exemple suivant :

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

Étape 6 Cliquez sur **Envoyer toutes les modifications**.

Étape 7 Observez la trace syslog pour vous assurer que la resynchronisation a réussi.

Étape 8 Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Étape 9 Sélectionnez **Voix -** > **Mise à disposition**.

Étape 10 Vérifiez que le paramètre GPP_D contient les informations que le script a capturé.

Ces informations comprennent le nom du produit, l'adresse MAC et le numéro de série si le périphérique de test exécute un certificat unique du fabricant. Les informations contiennent des chaînes génériques si l'unité a été fabriquée avant la version 2.0 du micrologiciel.

Un script similaire peut déterminer les informations sur le périphérique en cours de resynchronisation et ensuite fournir au périphérique les valeurs des paramètres de configuration appropriées.

Certificats HTTPS

Le téléphone fournit une stratégie de mise à disposition fiable et sécurisée qui repose sur les requêtes HTTPS de l'appareil au serveur de mise à disposition. Un certificat du serveur et un certificat client sont conjointement utilisés pour authentifier le téléphone sur le serveur et le serveur au téléphone.

Pour utiliser la fonctionnalité HTTPS avec le téléphone, vous devez générer une demande de signature de certificat (CSR) et l'envoyer à Cisco. Le téléphone génère un certificat pour installation sur le serveur de configuration. Le téléphone accepte le certificat lorsqu'il cherche à établir une connexion HTTPS avec le serveur de mise à disposition.

Méthodologie HTTPS

HTTPS crypte les communications entre un client et un serveur, protégeant ainsi le contenu du message vis-a-vis des autres périphériques réseau. La méthode de chiffrement pour le corps de la communication entre un client et un serveur est basée sur la cryptographie symétrique. La cryptographie symétrique, un client et un serveur partagent une seule clé secrète via un canal sécurisé qui est protégé par le chiffrement de clés publique/privée.

Les messages chiffrés à l'aide de la clé secrète peuvent être déchiffrés au moyen de la même clé. HTTPS prend en charge une large gamme d'algorithmes de chiffrement symétrique. Le téléphone met en œuvre un chiffrement symétrique jusqu'à 256 bits à l'aide de la norme de chiffrement américaine (AES), en plus du RC4 128 bits.

HTTPS fournit également l'authentification d'un serveur et d'un client engagés dans une transaction sécurisée. Cette fonction permet de s'assurer que les identités d'un serveur de mise à disposition et d'un client individuel ne peuvent pas avoir été usurpées par d'autres périphériques du réseau. Cette fonctionnalité est essentielle dans le cadre de la mise à disposition d'un terminal distant.

L'authentification du serveur et du client est effectuée à l'aide du chiffrement de clé publique/privée avec un certificat qui contient la clé publique. Le texte qui est chiffré avec une clé publique ne peut être déchiffré que par sa clé privée correspondante (et vice versa). Le téléphone prend en charge l'algorithme Rivest-Shamir-Adleman (RSA) pour le chiffrement de clé publique/privée.

Certificat du serveur SSL

Chaque serveur de mise à disposition sécurisé émet un certificat SSL (Secure Sockets Layer), que Cisco signe directement. Le micrologiciel qui s'exécute sur le téléphone ne reconnaît comme valide qu'un certificat Cisco. Lorsqu'un client se connecte à un serveur à l'aide de HTTPS, il rejette tous les certificats de serveur qui ne sont pas signés par Cisco.

Ce mécanisme permet de protéger le fournisseur de services face à un éventuel accès non autorisé au téléphone, ou face à toute tentative d'usurpation du serveur de mise à disposition. Sans cette protection, un pirate peut être en mesure de remettre à disposition le téléphone, pour obtenir des informations de configuration ou utiliser un autre service VoIP. En l'absence de la clé privée correspondant à un certificat de serveur valide, le pirate ne peut pas établir la communication avec un téléphone.

Obtenir un certificat du serveur

Procédure

Étape 1 Contactez un technicien Cisco, qui vous assistera tout au long du processus de certification. Si vous ne travaillez pas avec un technicien en particulier, vous pouvez envoyer un courrier électronique à l'adresse ciscosb-certadmin@cisco.com.

Étape 2 Générez une clé privée à utiliser pour la demande de signature de certification (CSR). Cette clé est privée et vous ne devez pas la fournir au support technique Cisco. Utilisez la boîte à outils Open Source « openssl » pour générer la clé. Par exemple :

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

Étape 3 Générez une demande de signature de certification (CSR) qui contienne des champs permettant d'identifier votre organisation et votre emplacement. Par exemple :

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

Vous devez disposer des informations ci-dessous :

- Champ Sujet : saisissez un nom commun (CN) qui doit être une syntaxe de nom de domaine complet (FQDN). Pendant l'établissement de la liaison d'authentification SSL, le téléphone vérifie que le certificat reçu est en provenance de la machine qui l'a envoyé.
- Nom d'hôte du serveur : par exemple, provserv.domain.com.
- Adresse e-mail : saisissez une adresse e-mail afin que le service clientèle puisse vous contacter si nécessaire. Cette adresse e-mail est visible dans la demande de signature de certification (CSR).

Étape 4 Envoyez par e-mail la demande de signature de certification (CSR) (en format zip) à un technicien Cisco ou à l'adresse ciscosb-certadmin@cisco.com. Le certificat est signé par Cisco. Cisco envoie le certificat que vous pouvez installer sur votre système.

Certificat client

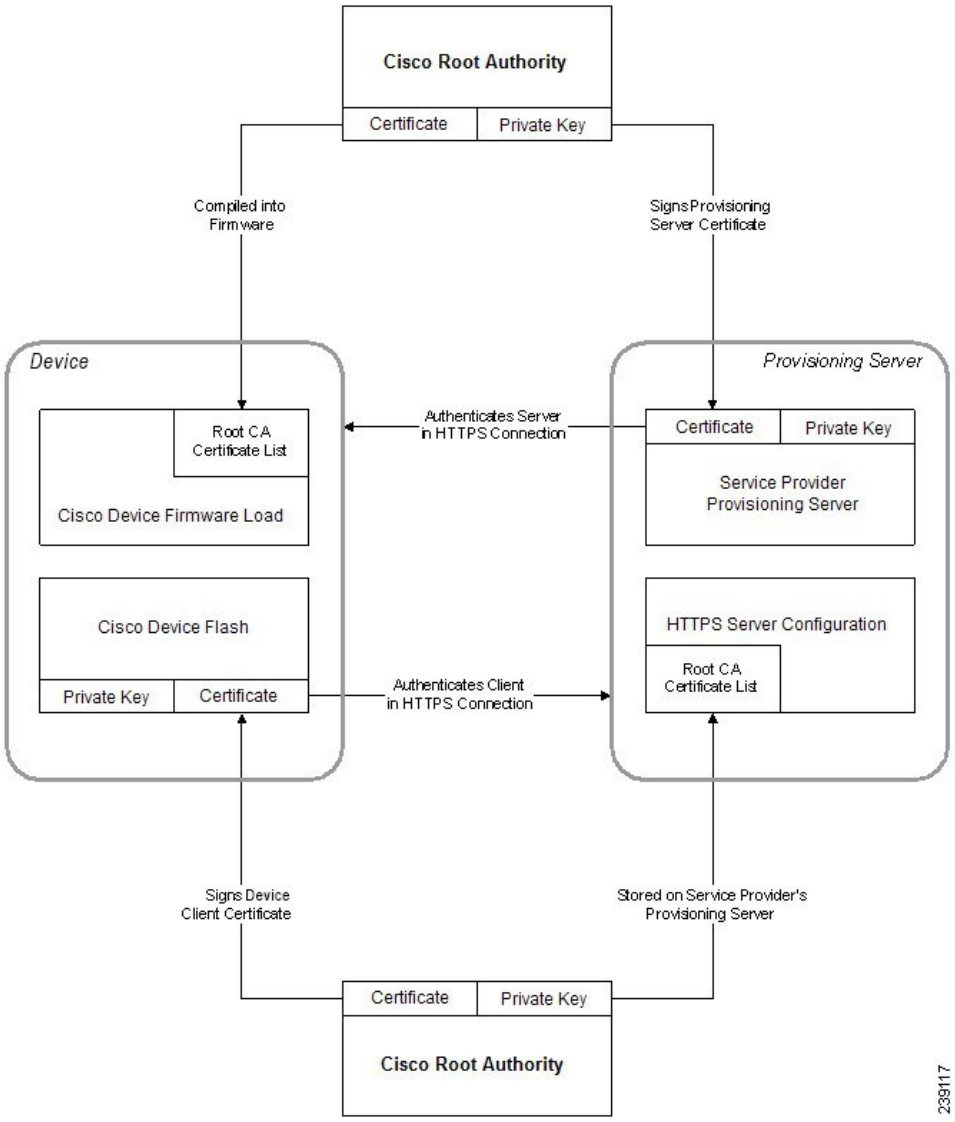
Outre une attaque directe sur le téléphone, un pirate pourrait essayer de contacter un serveur de mise à disposition à l'aide d'un navigateur Web standard ou d'un autre client HTTPS pour obtenir le profil de configuration présent sur le serveur de mise à disposition. Afin d'empêcher ce genre d'attaque, chaque téléphone dispose également d'un certificat client unique signé par Cisco, qui contient les informations d'identification relatives à chaque terminal individuel. Un certificat racine de l'Autorité de certification qui est capable d'authentifier le certificat client du périphérique est fourni à chaque fournisseur de services. Ce chemin d'authentification permet au serveur de mise à disposition de refuser les requêtes non autorisées pour des profils de configuration.

Structure du certificat

La combinaison d'un certificat du serveur et d'un certificat client garantit une communication sécurisée entre un téléphone distant et un serveur de mise à disposition. La figure ci-dessous illustre la relation et le positionnement des certificats, les paires de clés publique/privée et des autorités de signature racines, entre le client Cisco, le serveur de mise à disposition et l'autorité de certification.

La moitié supérieure du diagramme montre l'autorité racine du serveur de mise à disposition qui est utilisée pour signer le certificat du serveur de mise à disposition individuel. Le certificat racine correspondant est compilé dans le micrologiciel, ce qui permet au téléphone d'authentifier les serveurs de mise à disposition autorisés.

Illustration 2 : Flux d'autorité de certification



Configurer une autorité de certification personnalisée

Des certificats numériques peuvent être utilisés pour authentifier les périphériques réseau et les utilisateurs du réseau. Ils peuvent être utilisés pour négocier des sessions IPSec entre les nœuds du réseau.

Un tiers utilise un certificat d'autorité de certification pour valider et authentifier les deux nœuds ou plus qui tentent de communiquer. Chaque nœud dispose d'une clé publique et privée. La clé publique crypte les données. La clé privée déchiffre les données. Étant donné que les nœuds ont obtenu leurs certificats à partir de la même source, ils sont sûrs de leurs identités respectives.

Le périphérique peut utiliser des certificats numériques fournis par une autorité de certification tierce (CA) pour authentifier les connexions IPSec.

Les téléphones prennent en charge un ensemble d'autorité de certification racine préchargé incorporé au micrologiciel :

- Certificat d'autorité de certification Cisco Small Business
- Certificat d'autorité de certification CyberTrust
- Certificat d'autorité de certification VeriSign
- Certificat d'autorité de certification racine Sipura
- Certificat d'autorité de certification racine Linksys

Avant de commencer

Accéder à la page web d'administration du téléphone. Reportez-vous à Accéder à la page web du téléphone, à la page 9.

Procédure

Étape 1 Sélectionnez **Infos** > **État**.

Étape 2 Faites défiler jusqu'à **État d'autorité de certification personnalisée** et examinez les champs suivants :

- État de mise à disposition d'autorité de certification personnalisée : indique l'état de mise à disposition.
  - Dernière synchronisation réussie le jj/mm/aaaa hh:mn:ss ; ou
  - Dernière synchronisation en échec le jj/mm/aaaa hh:mn:ss
- Informations d'autorité de certification personnalisée : affiche des informations sur l'autorité de certification personnalisée.
  - Installed : affiche “Valeur CN,” où “Valeur CN” est la valeur du paramètre CN du champ Subject du premier certificat.
  - Not Installed : affiché si aucun certificat d'autorité de certification n’est installé.

Gestion des profils

Cette section décrit la formation des profils de configuration lors de la préparation en vue du téléchargement. Pour expliquer les fonctionnalités, TFTP à partir d'un PC local est utilisé comme méthode de resynchronisation, bien que HTTP ou HTTPS puissent également être utilisés.

Compresser un profil ouvert avec Gzip

Un profil de configuration au format XML peut devenir très volumineux si le profil indique tous les paramètres individuellement. Pour réduire la charge sur le serveur de mise à disposition, le téléphone prend en charge la compression du fichier XML, en utilisant le format de compression que prend en charge l'utilitaire gzip (RFC 1951).

Remarque La compression doit précéder le chiffrement pour que le téléphone puisse reconnaître un profil XML compressé et chiffré.

En vue de l'intégration dans des solutions de serveur de mise à disposition back-end personnalisées, la bibliothèque de compression zlib open source peut être utilisée à la place de l'utilitaire gzip autonome pour effectuer la compression de profil. Toutefois, le téléphone s'attend à ce que le fichier contienne un en-tête gzip valide.

Procédure

Étape 1 Installez gzip sur l'ordinateur local.

Étape 2 Compressez le profil de configuration `basic.txt` (décrit à la section Resynchronisation TFTP, à la page 51) en appelant gzip à partir de la ligne de commande :

```
gzip basic.txt
```

Cela génère le fichier compressé `basic.txt.gz` .

Étape 3 Enregistrez le fichier `basic.txt.gz` dans le répertoire racine virtuel du serveur TFTP.

Étape 4 Modifiez le paramètre Profile_Rule sur le périphérique de test pour effectuer une resynchronisation au fichier compressé à la place du fichier XML d'origine, comme indiqué dans l'exemple suivant :

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

Étape 5 Cliquez sur **Envoyer toutes les modifications.**

Étape 6 Observez la trace syslog à partir du téléphone.

Une fois la resynchronisation terminée, le téléphone télécharge le nouveau fichier et l'utilise pour mettre à jour ses paramètres.

Rubriques connexes

Compression de profil ouvert, à la page 20

Chiffrer un profil avec OpenSSL

Un profil compressé ou non compressé peut être chiffré (Toutefois, un fichier doit être compressé avant d'être chiffré). Le chiffrement est utile lorsque la confidentialité des informations du profil pose un problème spécifique, par exemple lorsque le serveur TFTP ou HTTP est utilisé pour la communication entre le téléphone et le serveur de mise à disposition.

Le téléphone prend en charge le chiffrement de clé symétrique à l'aide de l'algorithme AES 256 bits. Ce chiffrement peut être effectué en utilisant le package OpenSSL open source.

Procédure

Étape 1 Installez OpenSSL sur un PC local. Cela peut nécessiter que l'application OpenSSL soit recompilée pour activer AES.

Étape 2 À l'aide du fichier de configuration `basic.txt` (décrit en Resynchronisation TFTP, à la page 51), générez un fichier chiffré avec la commande suivante :

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

Le fichier compressé `basic.txt.gz` qui a été créé dans Compresser un profil ouvert avec Gzip, à la page 65 peut également être utilisé, car le profil XML peut être compressé et chiffré.

Étape 3 Enregistrez le fichier chiffré `basic.cfg` dans le répertoire racine virtuel du serveur TFTP.

Étape 4 Modifiez le paramètre Profile_Rule sur le périphérique de test pour une resynchronisation avec le fichier chiffré à la place du fichier XML d'origine. La clé de chiffrement se fait connaître du téléphone grâce à l'option URL suivante :

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

Étape 5 Cliquez sur **Envoyer toutes les modifications**.

Étape 6 Observez la trace syslog à partir du téléphone.

Une fois la resynchronisation terminée, le téléphone télécharge le nouveau fichier et l'utilise pour mettre à jour ses paramètres.

Rubriques connexes

Chiffrement AES-256-CBC, à la page 21

Créer des profils partitionnés

Un téléphone télécharge plusieurs profils distincts au cours de chaque resynchronisation. Cette pratique permet de gérer différents types d'informations de profil sur des serveurs distincts et de maintenir des valeurs des paramètres de configuration communes distinctes des valeurs spécifiques du compte.

Procédure

Étape 1 Créez un nouveau profil XML, `basic2.txt`, qui spécifie une valeur pour un paramètre qui le distingue des exercices précédents. Par exemple, pour le profil `basic.txt`, ajoutez :

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

Étape 2 Stockez le profil `basic2.txt` dans le répertoire racine virtuel du serveur TFTP.

Étape 3 Laissez la première règle de profil des exercices précédents dans le dossier, mais configurez la deuxième règle de profil (Profile_Rule_B) de manière à pointer vers le nouveau fichier :

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

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Le téléphone effectue maintenant une resynchronisation pour les premiers et seconds profils, dans cet ordre, chaque fois qu'une opération de resynchronisation arrive à échéance.

Étape 5 Observez la trace syslog pour confirmer le comportement attendu.

Définir l'en-tête de confidentialité du téléphone

Un en-tête de confidentialité d'utilisateur dans le message SIP définit les besoins de confidentialité des utilisateurs à partir du réseau de confiance.

Vous pouvez définir la valeur de l'en-tête de confidentialité de l'utilisateur pour chaque poste de la ligne à l'aide d'une balise XML dans le fichier `config.xml`.

Les options d'en-tête de confidentialité sont :

- Désactivé (par défaut)
- aucun : l'utilisateur demande que le service de confidentialité n'applique aucune fonction de confidentialité à ce message SIP.
- en-tête : l'utilisateur a besoin d'un service de confidentialité pour masquer les en-têtes qui ne peuvent pas être supprimés des informations d'identification.
- session : l'utilisateur demande qu'un service de confidentialité assure l'anonymat des sessions.
- utilisateur : l'utilisateur demande un niveau de confidentialité uniquement de la part des intermédiaires.
- ID : l'utilisateur demande au système de remplacer l'identifiant par un autre qui ne révèle pas l'adresse IP ou le nom d'hôte.

Procédure

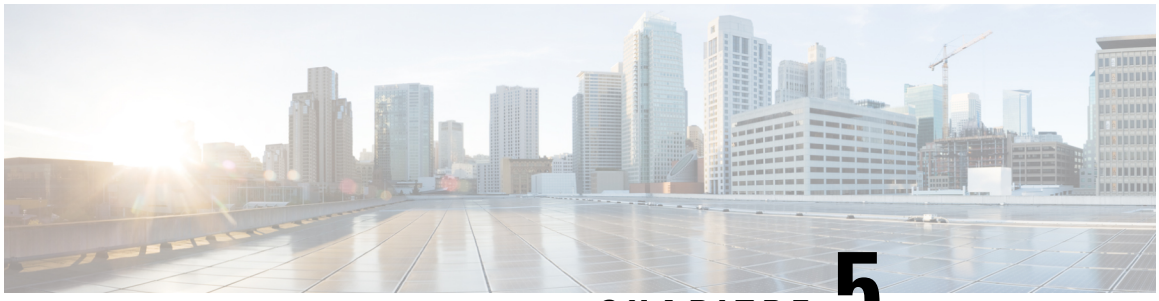
Étape 1 Modifiez le fichier `config.xml` du téléphone à l'aide d'un éditeur XML ou d'un éditeur de texte.

Étape 2 Insérez la valeur **<Privacy_Header_N_ ua="na">** ***de la balise*** **</Privacy_Header_N_>**, où N est le numéro de poste de la ligne (1 à 10) et utilisez l'une des valeurs suivantes.

- Valeur par défaut : **désactivé**
- **aucun**
- **en-tête**
- **session**
- **user**
- **id**

Étape 3 (facultatif) Mettez à disposition tous les numéros de poste de ligne supplémentaires à l'aide de la même balise avec le numéro de poste de ligne de votre choix.

Étape 4 Enregistrez les modifications apportées au fichier `config.xml`.



CHAPITRE 5

Paramètres de mise à disposition

Vue d'ensemble des paramètres de mise à disposition

Ce chapitre décrit les paramètres de mise à disposition qui peuvent être utilisés dans les scripts de profil de configuration.

Paramètres de profil de configuration

Le tableau ci-dessous indique la fonction et l'utilisation de chaque paramètre dans la section **Paramètres de profil de configuration** sous l'onglet **Mise à disposition**.

Nom paramètre	Description et valeur par défaut
Provision Enable	Contrôle toutes les actions de resynchronisation indépendamment des actions de mise à niveau du micrologiciel. Définir la valeur à **Oui** pour activer la mise à disposition à distance. La valeur par défaut est Oui.
Resync On Reset	Déclenche une resynchronisation après que chaque redémarrage à l'exception des redémarrages dus à des mises à niveau du micrologiciel et les mises à jour du paramètre. La valeur par défaut est Oui.

Nom paramètre	Description et valeur par défaut
Resync Random Delay	Délai aléatoire après la séquence de démarrage précédant la réinitialisation, indiqué en secondes. Dans un pool de périphériques de téléphonie IP planifiés pour un démarrage simultané, cette option permet d'espacer les heures auxquelles chaque unité envoie une requête de resynchronisation au serveur de mise à disposition. Cette fonctionnalité peut être utile dans les déploiements résidentiels de grande envergure, en cas de panne d'électricité régionale. La valeur de ce champ doit être un nombre entier compris entre 0 et 65 535. La valeur par défaut est de 2.
Resync At (HHmm)	L'heure (HHmn) à laquelle le périphérique se resynchronise avec le serveur de configuration. La valeur de ce champ doit être un nombre à quatre chiffres allant de 0000 à 2400 pour indiquer l'heure au format HHmn. Par exemple, 0959 indique 09:59. Aucune valeur par défaut n'est définie. Si la valeur n'est pas valide, le paramètre est ignoré. Si ce paramètre est défini à une valeur valide, le paramètre Resync Periodic est ignoré.
Resync At Random Delay	Empêche une surcharge du serveur de mise à disposition lorsqu'un grand nombre de périphériques sont mis en marche simultanément. Pour éviter de submerger le serveur de requêtes de resynchronisation à partir de plusieurs téléphones, le téléphone se resynchronise dans la plage comprise entre l'heure et les minutes et l'heure et les minutes plus le délai aléatoire (hhmm, hhmm + random_delay). Par exemple, si le délai aléatoire = (Resync At Random Delay + 30)/60minutes, la valeur d'entrée en secondes est convertie en minutes, arrondie à la minute supérieure pour calculer l'intervalle final random_delay. La valeur valide est comprise entre 0 et 65 535. Cette fonction est désactivée lorsque ce paramètre est défini sur zéro. La valeur par défaut est 600 secondes (10 minutes).

Nom paramètre	Description et valeur par défaut
Resync Periodic	L'intervalle de temps entre des resynchronisations périodiques avec le serveur de configuration. Le minuteur de resynchronisation associé est actif uniquement après la première synchronisation réussie avec le serveur. Les formats valides sont les suivants : • Un nombre entier Exemple : une entrée de **3000** indique que la resynchronisation suivante se produit dans 3000 secondes. • Plusieurs entiers Exemple : une entrée de **600,1200,300** indique que la première resynchronisation survient dans 600 secondes, la deuxième resynchronisation se produit dans 1200 secondes après la première, et la troisième resynchronisation dans 300 secondes après la deuxième. • Un intervalle de temps Par exemple, une entrée de **2400+30** indique que la resynchronisation suivante se produit entre 2400 et 2430 secondes après une resynchronisation réussie. Définissez ce paramètre à zéro pour désactiver la resynchronisation périodique. La valeur par défaut est de 3600 secondes.

Nom paramètre	Description et valeur par défaut
Resync Error Retry Delay	Si une resynchronisation échoue parce que le périphérique de téléphonie IP n'a pas pu récupérer un profil à partir du serveur, ou si le fichier téléchargé est endommagé ou si une erreur interne se produit, le périphérique tente à nouveau d'effectuer une resynchronisation après une heure spécifiée en secondes. Les formats valides sont les suivants : • Un nombre entier Exemple : une entrée de **300** indique que la prochaine tentative de resynchronisation se produit dans 300 secondes. • Plusieurs entiers Exemple : une entrée de **600,1200,300** indique que la première tentative survient de 600 secondes après l'échec, la deuxième tentative se produit 1200 secondes après l'échec de la première tentative, et la troisième tentative 300 secondes après l'échec de la deuxième tentative. • Un intervalle de temps Par exemple, une entrée de **2400+30** indique que la nouvelle tentative suivante se produit entre 2400 et 2430 secondes après un échec de resynchronisation. Si le délai est défini sur 0, le périphérique ne tente pas d'effectuer à nouveau une resynchronisation après une tentative de resynchronisation infructueuse.

Nom paramètre	Description et valeur par défaut
Forced Resync Delay	Délai maximum (en secondes) pendant lequel le téléphone attend avant d'effectuer une resynchronisation. Le périphérique n'effectue pas de resynchronisation lorsqu'une de ses lignes téléphoniques est active. Une resynchronisation pouvant prendre quelques secondes, il convient d'attendre que le périphérique soit resté inactif pendant une longue période avant de le resynchroniser. Cela permet de passer une succession d'appels sans interruption. L'appareil dispose d'un minuteur qui démarre le compte à rebours lorsque toutes les lignes sont inactives. Ce paramètre est la valeur initiale du compteur. Les événements de resynchronisation sont retardés jusqu'à ce que le compteur soit décrémenté jusqu'à zéro. La valeur valide est comprise entre 0 et 65 535. La valeur par défaut est de 14 400 secondes.
Resync From SIP	Permet à une resynchronisation d'être déclenchée via un message SIP NOTIFY. La valeur par défaut est Oui.
Resync After Upgrade Attempt	Active ou désactive l'opération de resynchronisation après qu'une mise à niveau se produit. Si Oui est sélectionné, la synchronisation est déclenchée. La valeur par défaut est Oui.
Resync Trigger 1, Resync Trigger 2	Conditions de déclenchement de resynchronisation pouvant être configurées. Une resynchronisation est déclenchée lorsque l'équation logique de ces paramètres est égale à TRUE. La valeur par défaut est (vide).
Resync Fails On FNF	Une resynchronisation est considérée comme ayant échoué si un profil requis n'est pas reçu du serveur. Ceci peut être annulé par ce paramètre. Lorsque cette option est définie sur **non**, le périphérique considère la réponse `file-not-found` du serveur comme une resynchronisation réussie. La valeur par défaut est Oui.

Nom paramètre	Description et valeur par défaut
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Chaque règle de profil informe le téléphone de l'existence d'une source à partir de laquelle obtenir un profil (fichier de configuration). Au cours de chaque opération de resynchronisation, le téléphone applique tous les profils de séquence. Par défaut : **`/$PSN.xml`** Si vous appliquez le chiffrement AES-256-cipher pour les fichiers de configuration, spécifiez la clé de chiffrement avec le mot-clé **`-clé`** en procédant comme suit : **`[--key <clé de chifrement>]`** Vous pouvez placer la clé de chiffrement entre guillemets doubles (") de manière optionnelle.
DHCP Option To Use	Options DHCP, délimitées par des virgules, utilisées pour récupérer le micrologiciel et les profils. La valeur par défaut est de 66,160,159,150,60,43,125.
Log Request Msg	Ce paramètre contient le message qui est envoyé au serveur syslog au début d'une tentative de resynchronisation. La valeur par défaut est `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`.
Log Success Msg	Message syslog qui émis à la fin d'une tentative réussie de resynchronisation. La valeur par défaut est `$PN $MAC –Successful Resync % $SCHEME://$SERVIP:$PORT$PATH -- $ERR`.
Log Failure Msg	Message syslog émis après une tentative de resynchronisation infructueuse. La valeur par défaut est `$PN $MAC -- Resync failed: $ERR`.
User Configurable Resync	Permet à l'utilisateur de resynchroniser le téléphone à partir de l'écran du téléphone IP. La valeur par défaut est Oui.

Paramètres de mise à niveau du micrologiciel

Le tableau ci-dessous indique la fonction et l'utilisation de chaque paramètre dans la section **Mise à niveau du micrologiciel** de l'onglet **Mise à disposition**.

Nom paramètre	Description et valeur par défaut
Upgrade Enable	Permet les opérations de mise à niveau du micrologiciel indépendamment des actions de resynchronisation. La valeur par défaut est Oui.
Upgrade Error Retry Delay	L'intervalle pour réessayer la mise à niveau (en secondes) s'applique lorsque la mise à niveau échoue. Le périphérique dispose d'un temporisateur d'erreur de mise à niveau du micrologiciel qui s'active après l'échec d'une tentative de cette mise à niveau. Le temporisateur est initialisé avec la valeur configurée dans ce paramètre. La prochaine tentative de mise à niveau du micrologiciel sera effectuée lorsque le décompte de ce temporisateur arrivera à zéro. La valeur par défaut est de 3600 secondes.
Upgrade Rule	Un script de mise à niveau du micrologiciel définit les conditions de la mise à niveau et les adresses URL associées du micrologiciel. Il utilise la même syntaxe que le paramètre Profile Rule. Utilisez le format qui suit pour saisir la règle de mise à niveau : **<tftp|http|https>://<adresse ip>/image/<nom de téléchargement>** Par exemple : **tftp://192.168.1.5/image/sip68xx.11-0-1MPP-BN.loads** Lorsqu'aucun protocole n'est spécifié, le protocole par défaut est TFTP. Si aucun nom de serveur n'est spécifié, l'hôte sollicitant l'URL est utilisé en tant que nom de serveur. Lorsqu'aucun port n'est spécifié, le port par défaut est utilisé (69 pour TFTP, 80 pour HTTP ou 443 pour HTTPS). La valeur par défaut est vide.
Log Upgrade Request Msg	Le message syslog émis au début d'une tentative de mise à niveau du micrologiciel. Valeur par défaut : `$PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH`
Log Upgrade Success Msg	Le message syslog émis après une tentative réussie de mise à niveau du micrologiciel. La valeur par défaut est `$PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR`

Nom paramètre	Description et valeur par défaut
Log Upgrade Failure Msg	Le message syslog émis après l'échec d'une tentative de mise à niveau du micrologiciel. La valeur par défaut est `$PN $MAC -- Upgrade failed: $ERR`
Peer Firmware Sharing	Active ou désactive la fonction Partage du micrologiciel avec les homologues. Sélectionnez **Oui** ou **Non** pour activer ou désactiver la fonction. Par défaut : Oui
Peer Firmware Sharing Log Server	Indique l'adresse IP et le port auxquels le message UDP est envoyé. Par exemple : 10.98.76.123:514 où, 10.98.76.123 est l'adresse IP et 514 est le numéro de port.

Paramètres généraux

Le tableau ci-dessous indique la fonction et l'utilisation de chaque paramètre dans la section **Paramètres généraux** de l'onglet **Mise à disposition**.

Nom paramètre	Description et valeur par défaut
GPP A - GPP P	Les paramètres à usage global GPP _* sont utilisés dans une chaîne libre enregistrée lors de la configuration des téléphones pour interagir avec un serveur de mise à disposition donné. Ils peuvent être configurés pour obtenir diverses valeurs, notamment les suivantes : • Des clés de chiffrement. • Des URL. • Des informations sur l'état d'une mise à disposition en plusieurs étapes. • Des modèles d'envoi de requête. • Des mappages d'alias de nom de paramètre. • Des valeurs de chaîne partielles, pouvant être combinées en des valeurs de paramètre complètes. La valeur par défaut est vide.

Variables d'expansion de macro

Certaines variables de macro sont reconnues dans les paramètres de mise à disposition suivants :

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_* (dans des conditions spécifiques)

Au sein de ces paramètres, les types de syntaxe, par exemple $NAME ou $(NAME), sont reconnus et font l'objet d'expansion.

Des sous-chaînes de variables macro peuvent être spécifiées avec la notation $$(NAME:p) et $(NAME:p:q), où p et q sont des entiers non négatifs (disponibles dans la révision 2.0.11 et supérieure). Le développement de macro qui en résulte est la sous-chaîne commençant au décalage de caractère p, de la longueur q (ou sinon jusqu'à la fin de la chaîne si q n'est pas spécifié). Par exemple, si GPP_A contient ABCDEF, alors $(A:2) prend la valeur étendue CDEF, et $(A:2:3) prend la valeur étendue CDE.

Un nom non reconnu n'est pas traduit, et la forme $NAME ou $(NAME) demeure inchangée dans la valeur du paramètre après expansion.

Nom paramètre	Description et valeur par défaut
$	La forme $$ se modifie pour devenir un seul caractère $.
A à P	Remplacé par le contenu des paramètres généraux GPP_A jusqu'à GPP_P.
SA à SD	Remplacés par les paramètres spéciaux GPP_SA à GPP_SD. Ces paramètres contiennent des clés ou des mots de passe utilisés lors de la mise à disposition. **Remarque** Les paramètres $SA à $SD sont reconnus comme des arguments pour l'identificateur d'URL de resynchronisation facultatif --key.
MA	L'adresse MAC utilisant des chiffres hexadécimaux en minuscules, par exemple 000e08aabbcc.
MAU	Adresse MAC utilisant des chiffres hexadécimaux en majuscules, par exemple 000E08AABBCC.

Nom paramètre	Description et valeur par défaut
MAC	Adresse MAC utilisant des chiffres hexadécimaux minuscules et des deux-points pour séparer les paires de chiffres hexadécimaux. Par exemple 00:0e:08:aa:bb:cc.
PN	Nom du produit. Par exemple, CP-6841-3PCC.
PSN	Numéro de série du produit. Par exemple, 6841-3PCC.
NS	Chaîne de numéro de série, par exemple 88012BA01234.
CCERT	État du certificat Client SSL : Installé ou Non installé.
IP	Adresse IP du téléphone au sein de son sous-réseau local. Par exemple 192.168.1.100.
EXTIP	Adresse IP externe du téléphone, comme illustré sur Internet. Par exemple 66.43.16.52.
SWVER	Chaîne de version du logiciel. Par exemple, sip68xx.11-0-1MPP.
HWVER	Chaîne de version du matériel. Par exemple, 2.0.1
PRVST	État de mise à disposition (une chaîne numérique) : -1 = requête de resynchronisation explicite 0 = resynchronisation de démarrage 1 = resynchronisation périodique 2 = la resynchronisation a échoué, nouvelle tentative
UPGST	État de mise à niveau (une chaîne numérique) : 1 = première tentative de mise à niveau 2 = la mise à niveau a échoué, nouvelle tentative
UPGERR	Message de résultat (ERR) de la tentative précédente de mise à niveau ; par exemple http_get a échoué.
PRVTMR	Secondes depuis la dernière tentative de resynchronisation.
UPGTMR	Secondes depuis la dernière tentative de mise à niveau.
REGTMR1	Secondes depuis que ligne 1 a perdu l'enregistrement sur le serveur SIP.
REGTMR2	Secondes depuis que ligne 2 a perdu l'enregistrement sur le serveur SIP.
UPGCOND	Nom de la macro existante.

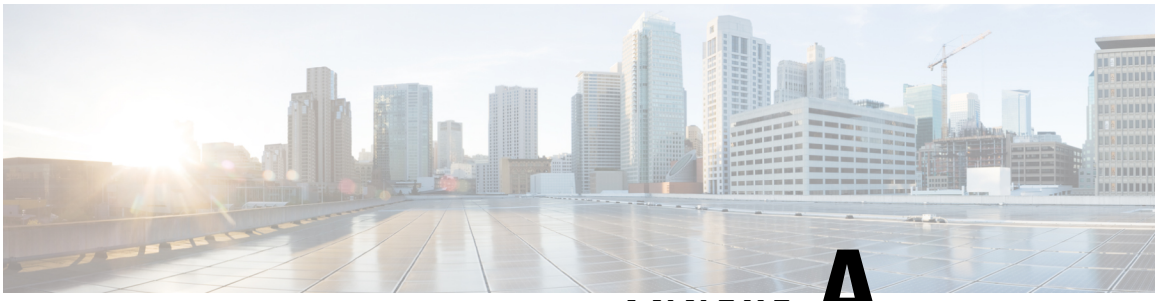
Nom paramètre	Description et valeur par défaut
SCHEME	Schéma d'accès au fichier, un parmi TFTP, HTTP ou HTTPS, comme obtenu après l'analyse de l'URL de mise à niveau ou de resynchronisation.
SERV	Demander le nom d'hôte du serveur cible, extrait après l'analyse de l'URL de resynchronisation ou de mise à niveau.
SERVIP	Demander l'adresse IP du serveur cible, extrait après l'analyse de l'URL de resynchronisation ou de mise à niveau, éventuellement suite à la recherche DNS.
PORT	Demander le port UDP/TCP cible, extrait après l'analyse de l'URL de resynchronisation ou de mise à niveau.
PATH	Demander le chemin du fichier cible, extrait après l'analyse de l'URL de resynchronisation ou de mise à niveau.
ERR	Message de résultats de la tentative de resynchronisation ou de mise à niveau. Utile uniquement pour générer les messages syslog de résultat. La valeur est conservée dans la variable UPGERR dans le cas des tentatives de mise à niveau.
UIDn	Le contenu du paramètre de configuration de l'ID utilisateur de la ligne n.
EMS	État Extension Mobility
MUID	ID utilisateur Extension Mobility
MPWD	Mot de passe Extension Mobility

Codes d'erreur interne

Le téléphone définit un certain nombre de codes d'erreur interne (X00 - X99) pour faciliter la configuration en fournissant un meilleur contrôle du comportement de l'unité sous certaines conditions d'erreur.

Nom paramètre	Description et valeur par défaut
X00	Erreur de couche de transport (ou ICMP) lors de l'envoi d'une requête SIP.
X20	La requête SIP expire lors de l'attente d'une réponse.
X40	Erreur générale du protocole SIP (par exemple, codec inacceptable dans SDP en 200 et messages ACK ou expiration en attendant ACK).

Nom paramètre	Description et valeur par défaut
X60	Numéro composé non valide conformément aux instructions du plan de numérotation fourni.



ANNEXE A

Exemple de profils de configuration

Exemple de Format Open XML

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

Exemple de profils de configuration

```
<!--  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>
<!--
```

Exemple de profils de configuration

```
 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
```

```
</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>
```

Exemple de profils de configuration

```
<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  -->
```

```
<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
-->
```

Exemple de profils de configuration

```
<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_>
```

Exemple de profils de configuration

```
<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  -->
```

Exemple de profils de configuration

```
<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_>
```

Exemple de profils de configuration

```
<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"/>
```

Exemple de profils de configuration

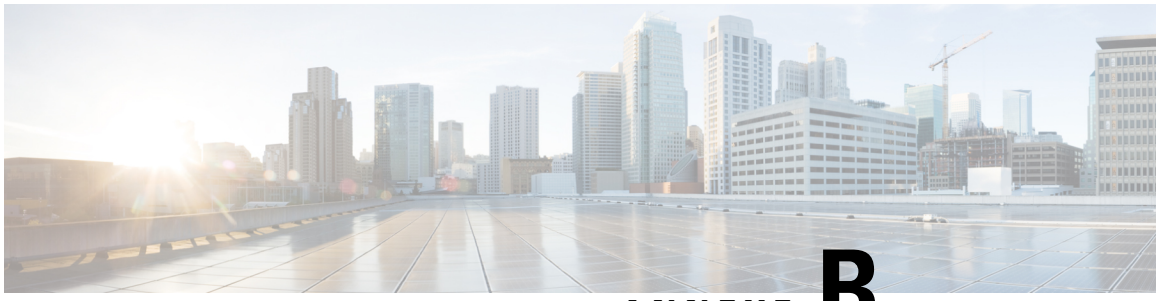
```
 <!--  <Login_Password_4_ ua="na"/>  -->
<Anywhere_Enable_4_ ua="na">No</Anywhere_Enable_4_>
<Block_CID_Enable_4_ ua="na">No</Block_CID_Enable_4_>
<DND_Enable_4_ ua="na">No</DND_Enable_4_>
<CFWD_Enable_4_ ua="na">No</CFWD_Enable_4_>
 <!--  Audio Configuration  -->
<Preferred_Codec_4_ ua="na">G711u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

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

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

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

Exemple de profils de configuration



ANNEXE B

Acronymes

Acronymes

CA	Courant alternatif
ACS	Serveur ACS
A/N	Convertisseur analogique numérique
AES	Advanced Encryption Standard
ANC	Appel anonyme
AP	Point d’accès
ASCII	American Standard Code for Information Interchange
B2BUA	Agent utilisateur verso
FLO	Supervision de ligne occupée
Bool	Valeurs booléennes. Spécifié comme Oui et Non, ou 1 et 0 dans le profil
BootP	Protocole Bootstrap
CA	Autorité de certification
CAS	Signal d'alerte CPE
CDP	Protocole CDP (Cisco Discovery Protocol)
CDR	Enregistrement détaillé des appels
CGI	Mmagery générée par l'ordinateur
CID	Affichage de l'ID de l'appelant
CIDCW	Appel en attente d'ID de l'appelant

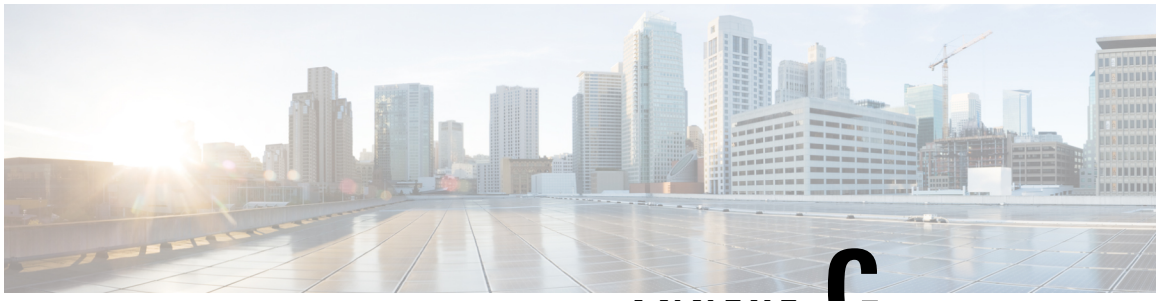
CNG	Services CNG (Comfort Noise Generation)
CPC	Contrôle du tiers appelant
CPE (Installations d'abonnés)	Installations d'abonnés
CSV	Valeurs séparées par des virgules
CWCID	Appel en attente d'ID de l'appelant
FORMAT CWT	Tnalité d'attente d'appel
N/A	Convertisseur numérique analogique
dB	Décibel
dBm	dB par rapport à 1 milliwatt
DHCP	Protocole DHCP (Dynamic Host Configuration Protocol)
NPD	Ne pas déranger
DNS	Système de noms de domaine
DoS	Déni de service
DRAM	Mémoire vive dynamique
DSL	Boucle d'abonné numérique
DSP	Digital Signal Processor - Processeur de signal numérique
heure d'été	Heure d'été
DTAS	Signal d'alerte de terminal de données (identique à CAS)
DTMF (Dual Tone Multi-Frequency)	Fréquence multiple à double tonalité
FQDN	Nom de domaine complet
FSK	Modulation par déplacement de fréquence
Pare-feu	Micrologiciel
FXS	Poste de change
GMT	temps moyen de Greenwich
GW	Passerelle

HTML (langage hypertexte)	Langage hypertexte
HTTP (Protocole de transfert hypertexte)	Protocole de transfert hypertexte
HTTPS	HTTP sur SSL
ICMP	Protocole ICMP (Internet Control Message Protocol)
IGMP	Internet Group Management Protocol
ILEC	Opérateur d'échange local titulaire
IP	Protocole Internet
IPv4	Version 4 du protocole IP
IPv6	Version 6 du protocole IP
ISP	Fournisseur d'accès à Internet
ITSP	Fournisseur de services de téléphonie Internet
UIT	International Telecommunication Union (Union internationale des télécommunications ou UIT)
IVR	Réponse vocale interactive
LAN	Réseau local
LBR	Bas débit
LBRC	Codec de bas débit
LCD	Affichage à cristaux liquides ; également appelé écran
LDAP	Lightweight Directory Access Protocol - Protocole LDAP
LED	Diode électroluminescente
Adresse MAC	adresse Media Access Control
MC	Certificat mini
MGCP	Protocole de contrôle de passerelle de média.
Attente musicale	Musique d'attente (MoH)
MOS	Note moyenne d'opinion (1 à 5, plus la note est élevée, meilleure elle est)

MPP	Téléphones multiplateformes
ms	Milliseconde
MSA	Adaptateur de source de musique
MWI	Indication des messages en attente
NAT (Traduction d'adresses de réseau)	Traduction d'adresses de réseau
NPS	Serveur de mise à disposition normale
NTP	Protocole Network Time (NTP)
OOB	Hors bande
OSI	Intervalle de commutation ouvert
PBX	Commutateur privé
PCB	Carte de circuits imprimés
PoE	L'alimentation PoE (Power over Ethernet)
PR	Inversion de la polarité
PS	Serveur de mise à disposition
PSQM	Mesure de la qualité vocale perçue (1 à 5, plus la note est basse, meilleure elle est)
PSTN	Réseau téléphonique public commuté
QoS	Qualité de service
RC	Supprimer la personnalisation
REQT	(SIP) Message de requête
RESP	(SIP) Message de réponse
RSC	(SIP) Code d'état de réponse, tels que 404, 302, 600
RTP (Real-Time Transport Protocol)	Protocole en temps réel
RTT	Durée de transmission ou RTT
SAS	Streaming Audio Server
SDP	Protocole SDP (Session Description Protocol)

SDRAM	DRAM synchrone
s	Secondes
SIP	Protocole SIP
SLA	Apparence de la ligne partagée
SLIC	Circuit d'interface de lignes d'abonnés (SLIC)
SP	Fournisseur de service
SSL (protocole SSL)	Secure Socket Layer
STUN	Session Traversal UDP for NAT
TCP	Protocole TCP (Transmission Control Protocol)
TFTP	Protocole TFTP (Trivial File Transfer Protocol)
TLS	Transport Layer Security
TTL	Durée de vie
ToS	Type de service
UA	Agent utilisateur
uC	Micro-contrôleur
UDP	Protocole UDP (User Datagram Protocol)
URI	URI (Uniform Resource Identifier)
URL	Uniform Resource Locator
UTC	Temps Universel Coordonné (UTC)
VAR	Revendeur à valeur ajoutée
VLAN	LAN vocal
VM	Messagerie vocale
VMWI	Indicateur visuel de message en attente
VoIP	Voix sur protocole Internet
VQ	Qualité voc.
WAN (réseau étendu)	Réseau étendu
XML	Extensible Markup Language

Acronymes



ANNEXE C

Documentation associée

Documentation associée

Consultez les sections suivantes pour obtenir des informations associées.

Documentation du téléphone IP Cisco 6800

Consultez les publications propres à votre langue, au modèle du téléphone et à la version du micrologiciel multiplateforme. Accédez à partir de l'URL (Uniform Resource Locator) suivante :

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

Politique de support des micrologiciels de téléphones IP Cisco

Pour plus d'informations sur la politique de support des téléphones, reportez-vous à https://cisco.com/go/phonefirmwaresupport.