Méthodes de mise à disposition

Mettre à disposition un téléphone à l'aide d'un serveur BroadSoft

Utilisateur du serveur BroadSoft uniquement.

Vous pouvez enregistrer vos téléphones multiplateformes IP Cisco sur une plate-forme BroadWorks.

Procédure

Étape 1 Téléchargez le kit CPE à partir de BroadSoft Xchange. Pour obtenir les kits CPE les plus récents, rendez-vous à l'adresse suivante : https://xchange.broadsoft.com.

Étape 2 Téléchargez le fichier DTAF le plus récent vers le serveur BroadWorks (Niveau système).

Pour plus d'informations, rendez-vous àl'adresse suivante : (https://xchange.broadsoft.com/node/1031047). Accédez au *Guide de configuration du partenaire BroadSoft* et reportez-vous à la section "*Configurer le type de profil de périphérique BroadWorks*".

Étape 3 Configurez le type de profil de périphérique BroadWorks.

Pour plus d'informations sur la configuration du type de profil de périphérique, accédez à l'URL suivante :

https://xchange.broadsoft.com/node/1031047. Accédez au *Guide de configuration du partenaire BroadSoft* et reportez-vous à la section "*Configuration du type de profil de périphérique BroadWorks*".

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.

Resynchronisation de base

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

Utilisez Syslog pour journaliser les messages

Un téléphone peut être configuré pour envoyer des messages de journalisation à un serveur Syslog via UDP, y compris les messages relatifs à la mise à disposition. Pour identifier ce serveur, vous pouvez accéder à l'interface Web du téléphone (voir Accéder à l'interface Web du téléphone), 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.

Pour obtenir les informations, vous pouvez accéder à l'interface Web du téléphone, sélectionnez **Info** > **Infos de déboguage** > **Journaux de contrôle** et cliquez sur **messages**.

Avant de commencer

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 3.

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.

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 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.

Messages de journal vers le serveur Syslog

Si un serveur syslog est configuré sur le téléphone grâce à l'utilisation des paramètres, 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).

Vous pouvez également configurer les paramètres dans le fichier de configuration du téléphone avec le code XML(cfg.xml). Pour configurer chaque paramètre, reportez-vous à la syntaxe de la chaîne dans Paramètres des journaux système, à la page 5.

Avant de commencer

- Un serveur Syslog est installé et configuré.
- Accéder à la page Web d'administration du téléphone. Reportez-vous à Accéder à l'interface Web du téléphone.

Procédure

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

Étape 2 Dans la section **Configuration réseau facultative**, entrez l'adresse IP du serveur dans **Serveur Syslog** et spécifiez éventuellement un **Identifiant Syslog** comme défini dans Paramètres des journaux système, à la page 5.

Étape 3 Si vous le souhaitez, vous pouvez définir le contenu des messages Syslog en utilisant **Journaliser le message de demande**, **Journaliser le message de réussite** et **Journaliser le message d'échec**, comme indiqué en Paramètres des journaux système, à la page 5.

Les champs définissant le contenu du message Syslog sont situés dans la section **Profil de configuration** de l'onglet **Voix** > **Mise à disposition**. Si vous ne spécifiez pas le contenu du message, les paramètres par défaut des champs sont utilisés. Si un champ est effacé, le message syslog correspondant n'est pas généré.

Étape 4 Cliquez sur **Envoyer toutes les modifications** pour appliquer la configuration.

Étape 5 Vérifier la validité de la configuration

a) Effectuez une resynchronisation TFTP. Reportez-vous à Resynchronisation TFTP, à la page 3.

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.

b) Vérifiez que votre serveur syslog a reçu des messages similaires aux messages suivants :

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt

CP-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

Paramètres des journaux système

Le tableau ci-dessous définit la fonction et l'utilisation des paramètres syslog dans la section **Configuration réseau facultative** sous l'onglet **Voix** > **Système** de l'interface Web du téléphone. Il définit également la syntaxe de la chaîne ajoutée au fichier de configuration du téléphone (cfg.xml) à l'aide du code XML pour configurer un paramètre.

Tableau 1 : Paramètres syslog

Nom paramètre	Description et valeur par défaut
Syslog Server	Cette fonctionnalité permet d'indiquer le serveur pour la journalisation des informations système et des événements essentiels du téléphone. Si les serveurs de débogage et syslog sont indiqués, les messages Syslog sont également consignés dans le serveur de débogage. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Syslog_Server ua="na">10.74.30.84</Syslog_Server>` • **Sur la page Web du téléphone**, spécifiez le serveur Syslog.

Nom paramètre	Description et valeur par défaut
Identificateur de syslog	Sélectionnez l'identificateur de périphérique à inclure dans les messages syslog qui sont téléchargées sur le serveur syslog. L'identificateur de périphérique s'affiche après l'horodatage de chaque message. Les options des identifiants sont les suivantes : • Aucun : aucun identificateur de périphérique. • $MA : l'adresse MAC du téléphone, exprimée sous forme de suite continue de minuscules et chiffres. Exemple : `c4b9cd811e29` • $MAU : l'adresse MAC du téléphone, exprimée sous forme de suite continue de majuscules et chiffres. Exemple : `C4B9CD811E29` • $MAC : l'adresse MAC du téléphone dans le format standard, séparée par des deux-points. Exemple : `c4:b9:cd:81:1e:29` • $SN : le numéro de série du téléphone. • **Dans le fichier de configuration du téléphone à l'aide de XML (**cfg.xml), entrez une chaîne au format suivant : `<Syslog_Identifier ua="na">$MAC</Syslog_Identifier>` • **Dans la page Web du téléphone**, sélectionnez un identificateur dans la liste. Par défaut : None
Log Request Msg	Message envoyé au serveur syslog au début d'une tentative de resynchronisation. Si aucune valeur n'est spécifiée, le message syslog n'est pas généré. La valeur par défaut est `$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH` • **Dans le fichier de configuration du téléphone à l'aide de XML (**cfg.xml), entrez une chaîne au format suivant : `<Log_Request_Msg ua="na">$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH</Log_Request_Msg>`
Log Success Msg	Message syslog qui est émis à la fin d'une tentative réussie de resynchronisation. Si aucune valeur n'est spécifiée, le message syslog n'est pas généré. **Dans le fichier de configuration du téléphone avec XML(cfg.xml)**, entrez une chaîne dans ce format : `<Log_Success_Msg ua="na">$PN $MAC -- Resynchronisation réussie $SCHEME://$SERVIP:$PORT$PATH</Log_Success_Msg>`
Log Failure Msg	Message syslog émis après une tentative de resynchronisation infructueuse. Si aucune valeur n'est spécifiée, le message syslog n'est pas généré. La valeur par défaut est `$PN $MAC -- Resync failed: $ERR` **Dans le fichier de configuration du téléphone avec XML(cfg.xml)**, entrez une chaîne dans ce format : `<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed : $ERR</Log_Failure_Msg>`

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 3. 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 référencés comme $A à $P. Pour obtenir la liste complète des variables disponibles pour l'expansion des macros, voir Variables d'expansion de macro.

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

Mettre 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 3) 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 l'interface Web du téléphone.

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.

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.

Resynchroniser avec 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 3) 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
```

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 l'interface Web du téléphone.

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 2).

Étape 6 Vérifiez que le champ **Resync lors de la réinitialisation** 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.

Paramètres de resynchronisation du profil

Le tableau suivant définit la fonction et l'utilisation des paramètres du profil de resynchronisation dans la section **Profil de configuration** sous l'onglet **Voix** > **Mise à disposition** de la page Web du téléphone. Il définit également la syntaxe de la chaîne ajoutée au fichier de configuration du téléphone (cfg.xml) à l'aide du code XML pour configurer un paramètre.

Paramètre	Description
Activation de la mise à disposition	Autorise ou refuse des actions de resynchronisation du profil. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Provision_Enable ua="na">Oui</Provision_Enable>` • **Sur la page Web du téléphone**, définissez ce champ sur **Oui** pour autoriser les actions de resynchronisation ou sur **Non** pour bloquer les actions de resynchronisation. Par défaut : Oui
Resync lors de la réinitialisation	Indique si le téléphone resynchronise les configurations avec le serveur de mise à disposition après la mise sous tension et après chaque nouvelle tentative de mise à niveau. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_On_Reset ua="na">Oui</Resync_On_Reset>` • **Sur la page Web du téléphone**, définissez ce champ sur **Oui** pour autoriser les actions de resynchronisation au démarrage ou lors d'une réinitialisation, ou sur **Non** pour bloquer les actions de resynchronisation dans ces deux cas. Par défaut : Oui

Paramètre	Description
Resync Random Delay	Empêche une surcharge du serveur de mise à disposition lorsqu'un grand nombre de périphériques sont mis en marche simultanément et tentent une configuration initiale. Ce délai ne prend effet que lors de la tentative de configuration initiale, après la mise sous tension ou la réinitialisation d'un périphérique. Il s'agit de l'intervalle de temps maximum pendant lequel le périphérique attend avant de prendre contact avec le serveur de mise à disposition. Le délai réel est un nombre pseudo-aléatoire compris entre 0 et cette valeur. Ce paramètre est en unités de 20 secondes. La valeur valide est comprise entre 0 et 65 535. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_Random_Delay ua="na">2</Resync_Random_Delay>` • **Sur la page Web du téléphone**, spécifiez le nombre d'unités (20 secondes) permettant au téléphone de retarder la resynchronisation après la mise sous tension ou la réinitialisation. La valeur par défaut est 2 (40 secondes).
Resync At (HHmm)	L'heure (HHMM) 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. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_At__HHmm_ ua="na">0959</Resync_At__HHmm_>` • **Sur la page Web du téléphone**, spécifiez l'heure au format HHMM à laquelle le téléphone doit démarrer la resynchronisation. 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.

Paramètre	Description
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. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>` • **Sur la page Web du téléphone**, spécifiez la période en secondes. La valeur valide est comprise entre 0 et 65 535. Si la valeur est inférieure à 600, le délai aléatoire interne se situe entre 0 et 600. La valeur par défaut est 600 secondes (10 minutes).
Resync Periodic	L'intervalle de temps entre des resynchronisations périodiques avec le serveur de mise à disposition. 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. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_Periodic ua="na">3600</Resync_Periodic>` • **Sur la page Web du téléphone**, spécifiez la période en secondes. Définissez ce paramètre à zéro pour désactiver la resynchronisation périodique. La valeur par défaut est de 3600 secondes.

Paramètre	Description
Resync Error Retry Delay	Si une resynchronisation échoue parce que le téléphone 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 téléphone 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. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_Error_Retry_Delay ua="na">60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400</Resync_Error_Retry_Delay>` • **Sur la page Web du téléphone**, spécifiez la période en secondes. Valeur par défaut : 60, 120, 240, 480, 960, 1920, 3840, 7680, 15360, 30720, 61440, 86400

Paramètre	Description
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. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Forced_Resync_Delay ua="na">14400</Forced_Resync_Delay>` • **Sur la page Web du téléphone**, spécifiez la période en secondes. La valeur par défaut est de 14 400 secondes.
Resync From SIP	Contrôle les requêtes de resynchronisation via un événement SIP NOTIFY envoyé par le serveur proxy du fournisseur de service au téléphone. Lorsqu'il est activé, le proxy peut demander une resynchronisation en envoyant au périphérique, un message SIP NOTIFY contenant l'en-tête Event: resync. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_From_SIP ua="na">Oui</Resync_From_SIP>` • **Sur la page Web du téléphone**, sélectionnez **Oui** pour activer cette fonction et cliquez sur **Non** pour la désactiver. Par défaut : 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 après une mise à niveau du micrologiciel. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_After_Upgrade_Attempt ua="na">Oui</Resync_After_Upgrade_Attempt>` • **Sur la page Web du téléphone**, sélectionnez **Oui** pour déclencher la resynchronisation après une mise à niveau du micrologiciel ou **Non** pour ne pas effectuer de resynchronisation. Par défaut : Oui

Paramètre	Description

Resync Trigger 1
Resync Trigger 2
	Si l'équation logique de ces paramètres a la valeur FALSE, la resynchronisation n'est pas déclenchée même lorsque **Resync lors de la réinitialisation** est défini sur **TRUE**. Seule la resynchronisation via l'URL d'action directe et la notification SIP ne tiennent pas compte de ces déclenchements de resynchronisation.
	Les paramètres peuvent être programmés avec une expression conditionnelle qui subit une expansion de macro. Pour les expansions de macro valides, reportez-vous à Variables d'expansion de macro.
	• **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant :
	`<Resync_Trigger_1 ua="na">$UPGTMR gt 300 and $PRVTMR ge 600</Resync_Trigger_1>`
	`<Resync_Trigger_2 ua="na"/>`
	• **Sur la page Web du téléphone**, spécifiez les déclencheurs.
	Par défaut : vide

User Configurable Resync	Permet à l'utilisateur de resynchroniser le téléphone à partir du menu de l'écran du téléphone. Lorsque ce paramètre est défini sur **Oui**, un utilisateur peut resynchroniser la configuration du téléphone en entrant la règle de profil à partir du téléphone. Lorsque cette valeur est définie sur **Non**, le paramètre de **règle de profi** ln'est pas affiché dans le menu de l'écran du téléphone. Le paramètre de **Règle de profil** est situé sous **Applications** > **Administration du périphérique**. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<User_Configurable_Resync ua="na">Oui</User_Configurable_Resync>` • **Sur la page Web du téléphone**, sélectionnez **Oui** pour afficher le paramètre de la **règle de profil**dans le menu du téléphone, ou sélectionnez **Non** pour masquer ce paramètre. Par défaut : Oui
Resync Fails On FNF	Une resynchronisation est généralement considérée comme ayant échoué si un profil demandé n'est pas reçu du serveur. Ce paramètre a la priorité sur ce comportement. Lorsque cette option est définie sur **Non**, le périphérique considère la réponse `file-not-found` du serveur comme une resynchronisation réussie. • **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant : `<Resync_Fails_On_FNF ua="na">Oui</Resync_Fails_On_FNF>` • **Sur la page Web du téléphone**, sélectionnez **Oui** pour accepter une réponse `fichier-introuvable` comme échec de resynchronisation, ou sélectionnez **non** pour accepter une réponse `fichier-introuvable` comme étant une resynchronisation réussie. Par défaut : Oui

Paramètre	Description

Type d'authentification de profil	Spécifie les informations de connexion à utiliser pour l'authentification de compte de profil. Les options disponibles sont les suivantes :
	• **Désactivé**: désactive la fonction de compte de profil. Lorsque cette fonction est désactivée, le menu **Configuration du compte de profil** ne s'affiche pas sur l'écran du téléphone.
	• **L'authentification de base HTTP** : les identifiants de connexion HTTP la sont utilisés pour authentifier le compte de profil.
	• **Authentification XSI** : informations d'identification de connexion XSI ou XSI SIP sont utilisés pour authentifier le compte de profil. Les informations d'authentification dépendent du **Type d'authentification XSI** du téephone :
	  • Lorsque le **Type d'authentification XSI** du téléphone est défini sur **Identifiants de connexion**, les informations d'identification de connexion XSI sont utilisées.
	  • Lorsque le **Type d'authentification XSI** du téléphone est défini sur **Informations d'identification SIP**, les informations d'identification XSI SIP sont utilisées.
	• **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant :
	`<Profile_Authentication_Type ua="na">Basic Http Authentication</Profile_Authentication_Type>`
	• **Sur la page Web du téléphone**, sélectionnez une option dans la liste pour la resynchronisation du profil du téléphone.
	Valeur par défaut : L'authentification HTTP

Paramètre	Description

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.
	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 <encryption key>]`
	Vous pouvez placer la clé de chiffrement entre guillemets doubles (") de manière optionnelle.
	• **Dans le fichier de configuration du téléphone à l'aide de XML (cfg.xml)**, entrez une chaîne au format suivant :
	`<Profile_Rule ua="na">/$PSN.xml</Profile_Rule>`
	`<Profile_Rule_B ua="na"/>`
	`<Profile_Rule_C ua="na"/>`
	`<Profile_Rule_D ua="na"/>`
	• **Sur la page Web du téléphone**, spécifiez la règle de profil.
	Par défaut : **`/$PSN.xml`**

DHCP Option To Use	Options DHCP, délimitées par des virgules, utilisées pour récupérer le micrologiciel et les profils. Par défaut : 66,160,159,150,60,43,125
DHCPv6 Option To Use	Options DHCP, délimitées par des virgules, utilisées pour récupérer le micrologiciel et les profils. Par défaut : 17 160 159

Configurer vos téléphones pour l'intégration via le code d'activation

Si votre réseau est configuré pour l'intégration par le code d'activation, vous pouvez configurer de nouveaux téléphones pour qu'ils s'inscrivent automatiquement de manière sécurisée. Vous générez et fournissez à chaque utilisateur un code d'activation unique à 16 chiffres. L'utilisateur saisit le code d'activation, et le téléphone s'enregistre automatiquement. Cette fonction garantit la sécurité de votre réseau, car le téléphone ne peut pas s'enregistrer tant que l'utilisateur n'a pas saisi de code d'activation valide.

Les codes d'activation ne peuvent être utilisés qu'une seule fois et ont une date d'expiration. Si un utilisateur saisit un code arrivé à expiration, le téléphone affiche `Code d'activation incorrect` à l'écran. Si cela se produit, fournissez un nouveau code à l'utilisateur.

Cette fonctionnalité est disponible dans le firmware 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. Pour ce faire, procédez comme suit.

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.

Si vous souhaitez configurer un serveur de proxy pour l'intégration, assurez-vous de le configurer correctement. Reportez-vous à Configurer un serveur de proxy.

Accéder à la page Web du téléphone Accéder à l'interface Web du téléphone

Procédure

Étape 1 Réinitialisez le téléphone avec les paramètres d'usine.

Étape 2 Sélectionnez **Voix** > **Mise à disposition** > **Profil de configuration**.

Étape 3 Entrez la règle de profil dans le champ **Règle de profil** comme décrit dans le tableau Paramètres de mise à disposition via le code d'activation, à la page 19

Étape 4 (Facultatif) Dans la section **Mise à niveau du micrologiciel**, saisissez la règle de mise à niveau dans le champ **Règle de mise à niveau** comme décrit dans le tableau Paramètres de mise à disposition via le code d'activation, à la page 19.

Étape 5 Envoyer toutes les modifications.

Paramètres de mise à disposition via le code d'activation

Le tableau suivant définit la fonction et l'utilisation des paramètres du code d'activation dans la section **Profil de configuration** sous l'onglet **Voix** > **Mise à disposition** de la page Web du téléphone. Il définit également la syntaxe de la chaîne ajoutée au fichier de configuration du téléphone (cfg.xml) à l'aide du code XML pour configurer un paramètre.

Paramètre	Description

Profile Rule
Profile Rule B
Profile Rule C
Profile Rule D
	Règles de profil de configuration à distance évaluées en séquence. Chaque resynchronisation peut récupérer plusieurs fichiers, potentiellement gérés par des serveurs distincts.
	Exécutez l'une des actions suivantes :
	• Dans le fichier de configuration du téléphone à l'aide de XML(cfg.xml), entrez une chaîne au format suivant :
	`<Profile_Rule ua="na">gds://</Profile_Rule>`
	• Dans l'interface Web du téléphone, entrez une chaîne au format suivant :
	`gds://`
	Par défaut : /$PSN.xml

Paramètre	Description

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.
	Exécutez l'une des actions suivantes :
	• Dans le fichier de configuration du téléphone à l'aide de XML(cfg.xml), entrez une chaîne au format suivant :
	`<Upgrade_Rule ua="na">http://<server ip address>/ sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>`
	• Dans l'interface Web du téléphone, saisissez la règle de mise à niveau :
	`protocol://server[:port]/profile_pathname`
	Par exemple :
	`tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.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).
	Par défaut : vide

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.

Authentifier à l'aide de la 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 3) 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 22.

HTTPS avec authentification par certificat client

Dans la configuration d'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.

Authentifier HTTPS 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 20.

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.

Configurer un serveur HTTPS pour le filtrage client et le 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 l'interface Web du téléphone.

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.

Outre les certifications émises par Cisco, le téléphone accepte également les certificats de serveur provenant d'un ensemble de fournisseurs de certificats SSL communément utilisés.

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-à-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 le CSR (au format de fichier zip) par courrier électronique au responsable de l'assistance Cisco ou à l'adresse suivante ciscosb-certadmin@cisco.com. Le certificat est signé par Cisco. Cisco envoie le certificat que vous pouvez installer sur votre système.

Certificat client

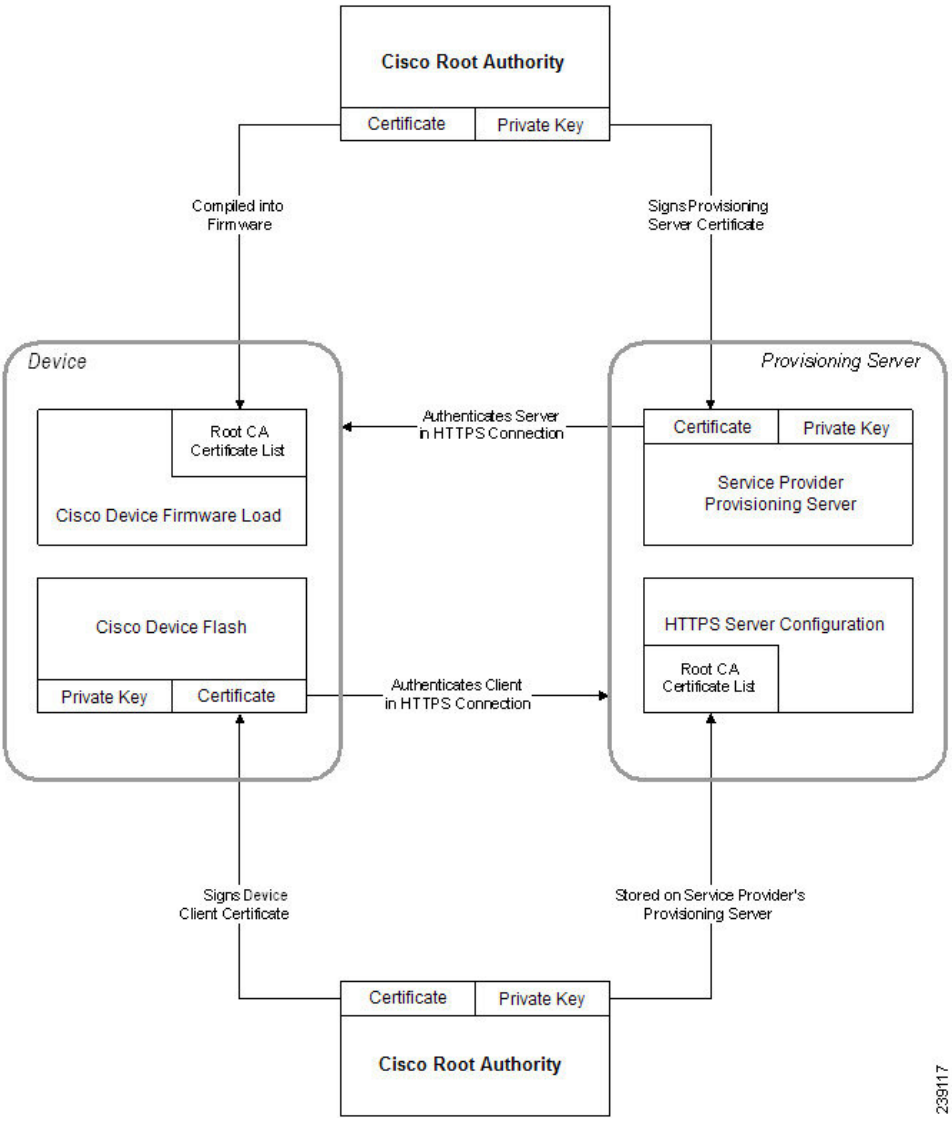
Outre une attaque directe sur le téléphone, un pirate pourrait essayer de contacter un serveur de mise à disposition à l'aide d'un navigateur Web standard ou d'un autre client HTTPS pour obtenir le profil de configuration présent sur le serveur de mise à disposition. Afin d'empêcher ce genre d'attaque, 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 1 : 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 l'interface Web du téléphone.

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 3) 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 **Submit All Changes (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.

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 3), 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 28 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.

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 balise **<Privacy_Header_N_ ua="na">*Value*</Privacy_Header_N_>**, où N est le numéro d'extension de la ligne (1-10), 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`.

Renouveler le certificat MIC

Vous pouvez renouveler le certificat installé par le fabricant (Manufacture Installed Certificate, MIC) à l'aide d'un service d'identification de périphérique unique sécurisé (SUDI) spécifié ou par défaut. Si le certificat MIC expire, les fonctionnalités qui utilisent SSL/TLS ne fonctionnent pas.

Avant de commencer

- Assurez-vous que vous autorisez le service `sudirenewal.cisco.com` (port 80) à traverser votre pare-feu pour prendre en charge le renouvellement de certificat MIC.
- Accéder à la page Web d'administration du téléphone. Reportez-vous à Accéder à l'interface Web du téléphone.

Procédure

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

Étape 2 Dans la section **Paramètres du Cert MIC**, définissez les paramètres comme indiqué dans Paramètres pour le renouvellement des certificats MIC par le service SUDI, à la page 32.

Étape 3 Cliquez sur **Envoyer toutes les modifications**.
Une fois le renouvellement du certificat terminé, le téléphone redémarre.

Étape 4 (Facultatif) Vérifiez l'état le plus récent du renouvellement de certificat MIC sous la **section état** d'actualisation du CERT du micro à partir de l' > **État de téléchargement info** .

Remarque Si vous restaurez les paramètres d'usine du téléphone, le téléphone utilise néanmoins toujours le certificat renouvelé.

Paramètres pour le renouvellement des certificats MIC par le service SUDI

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

Tableau 2 : Paramètres pour le renouvellement des certificats MIC par le service SUDI

Nom paramètre	Description et valeur par défaut
Activation de la mise à jour du Cert MIC	Contrôle l'activation du renouvellement du certificat installé par le fabricant (MIC) par le service Secure Unique Device Identifier (SUDI) par défaut ou spécifié. Exécutez l'une des actions suivantes : • Dans le fichier de configuration du téléphone à l'aide de XML(cfg.xml), entrez une chaîne au format suivant : `<MIC_Cert_Refresh_Enable ua="na">Yes</MIC_Cert_Refresh_Enable>` • Dans l'interface Web du téléphone, sélectionnez **Oui** ou **Non** pour activer ou désactiver le renouvellement du certificat MIC. Valeurs valides : Oui et Non Par défaut : Non

Règle d'actualisation du Cert. MIC	Saisissez l'URL HTTP du service SUDI qui fournit le certificat MIC renouvelé, par exemple,
	`http://sudirenewal.cisco.com/`
	Remarque Ne modifiez pas l'URL. Seule l'URL par défaut est prise en charge pour le renouvellement de certificat MIC.
	Exécutez l'une des actions suivantes :
	• Dans le fichier de configuration du téléphone à l'aide de XML(cfg.xml), entrez une chaîne au format suivant :
	`<MIC_Cert_Refresh_Rule ua="na">http://sudirenewal.cisco.com/</MIC_Cert_Refresh_Rule>`
	• Dans l'interface Web du téléphone, saisissez l'URL HTTP à utiliser.
	Valeurs autorisées : une URL valide ne dépassant pas 1024 caractères
	Valeur par défaut : `http://sudirenewal.cisco.com/`

Définir la règle de mise à niveau du casque Cisco

Vous pouvez mettre à niveau le micrologiciel d'un casque Cisco en le connectant à un téléphone IP Cisco multiplateforme. Avant que l'utilisateur n'effectue la mise à niveau, vous devez définir la règle de mise à niveau sur la page Web d'administration du téléphone. Lorsque le casque est connecté au téléphone, le téléphone détecte automatiquement la nouvelle version du micrologiciel du casque, puis invite l'utilisateur à effectuer la mise à niveau.

Les connexions prises en charge pour la mise à niveau sont les suivantes :

- Casque Cisco série 520 : câble USB
- Casque Cisco série 560 : câble USB et câble en Y (connecteur RJ-9 et AUX)

- Casque Cisco série 700 : câble USB

Les paramètres du casque ne sont pas effacés par une réinitialisation du téléphone. La règle de mise à niveau prend en charge les protocoles HTTP et TFTP.

La version du casque Cisco fournit le fichier XML du casque qui peut être utilisé pour la mise à niveau du micrologiciel. Si la version du logiciel dans le fichier est ultérieure au micrologiciel du casque, l'utilisateur est invité à mettre à niveau le casque sur l'écran du téléphone. L'utilisateur peut choisir de mettre à niveau le casque immédiatement ou remettre à une date ultérieure.

Avant de commencer

Accéder à la page Web d'administration du téléphone. Reportez-vous à Accéder à l'interface Web du téléphone.

Procédure

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

Étape 2 Sélectionnez le paramètre **Règle de mise à niveau de casque Cisco** qui se trouve à la section **Mise à niveau du micrologiciel de casque Cisco**.

Étape 3 Spécifiez le protocole TFTP, HTTP ou HTTPS, une adresse IP du périphérique de mise à niveau du casque et le nom du fichier XML du casque. Saisissez les valeurs en tant que chaîne unique dans le paramètre.

Mise en garde Ne modifiez pas le contenu du fichier XML du casque.

Par exemple, `tftp://10.74.51.81/prov/headset/1-6-0-162/ciscoheadsetfirmware.xml`

Vous pouvez également configurer ce paramètre dans le fichier de configuration (cfg.xml).

```
<Cisco_Headset_Upgrade_Rule
ua="na">tftp://10.74.51.81/prov/headset/1-6-0-162/ciscoheadsetfirmware.xml</Cisco_Headset_Upgrade_Rule>
```

Étape 4 Cliquez sur **Envoyer toutes les modifications**.
Lorsqu'une nouvelle version du micrologiciel du casque est détectée, le téléphone affiche une invite de mise à niveau.