# Mise à disposition



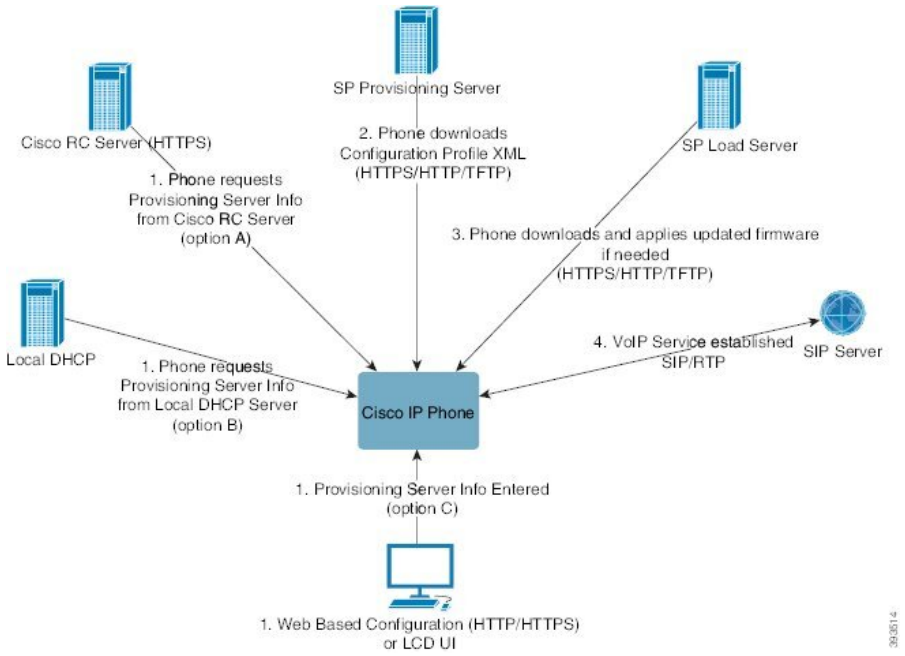
# Présentation de la mise à disposition

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. DNS SRV, GDS (intégration par code d'activation), l'activation du périphérique EDOS.
   - **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

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 11. 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.

## 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.

## Intégrer votre téléphone avec le code d'activation

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. 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.

### 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.

### 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>
```

**Remarque** Pour les versions du micrologiciel postérieures à 11.2(3) SR1, le paramètre de `mise à niveau du micrologiciel` est facultatif.

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

# Intégration du téléphone au Webex Cloud

l'intégration du téléphone constitue un moyen simple et sécurisé d'intégrer des téléphones compatibles Webex au Webex Cloud. Vous pouvez réaliser le processus d'intégration à l'aide de l'intégration via le code d'activation (GDS) ou de l'adresse MAC du téléphone (activation du périphérique EDOS).

Pour plus d'informations sur la façon de générer le code d'activation, reportez-vous au *Guide de configuration des partenaires Cisco BroadWorks, des téléphones multi-plateformes Cisco*.

Pour plus d'informations sur l'intégration de téléphones compatible Webex, reportez-vous au *Guide de la Solution Webex pour Cisco BroadWorks*.

# Activer un téléphone pour l'intégration au Webex Cloud

Après l'enregistrement réussi du téléphone dans le Webex Cloud, un symbole de nuage  apparaît sur l'écran du téléphone.

### 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** > **Téléphone**.

**Étape 2** Dans la section **Webex**, définissez le paramètre **Intégration activée** sur **Oui**.

Vous pouvez également configurer ce paramètre dans le fichier de configuration XML du téléphone (cfg.xml) en entrant une chaîne au format suivant :

```
<Webex_Onboard_Enable ua="na">Yes</Webex_Onboard_Enable>
```

Valeur par défaut: Oui

**Étape 3** Cliquez sur **Envoyer toutes les modifications**.

# Activer la mise à disposition automatique avec un code d'activation court

Utilisez les étapes ci-dessous pour activer la mise à disposition automatique avec un code d'activation court.

### Avant de commencer

Assurez-vous que vos téléphones sont mis à jour avec la version du micrologiciel 11.3(1) ou version ultérieure.

Si vous souhaitez partager un serveur de proxy pour le téléphone, assurez-vous que le serveur de proxy est configuré correctement. Reportez-vous à Configurer un serveur de proxy.

Vérifiez comment configurer le serveur CDA pour le profil de redirection :

https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244

### Procédure

**Étape 1** Créez un nom de profil de redirection qui contient un nombre illimité de chiffres entre trois et 16 inclus. Cela devient le code d'activation, ultérieurement. Utilisez l'un des formats suivants :

- `nnn`.
- `nnnnnnnnnnnnnnnn`
- N'importe quel nombre de chiffres entre trois et seize, inclus. Exemple, `123456`

**Étape 2** Fournissez le nom de profil que vous avez créé à l'étape 1 à l'équipe d'assistance Customer Device Activation (CDA) à l'adresse cdap-support@cisco.com.

**Étape 3** Demandez à l'équipe d'assistance CDA d'activer votre profil pour la découverte.

**Étape 4** Lorsque vous recevez une confirmation de la part de l'équipe d'assistance CDA, distribuez le code d'activation aux utilisateurs.

**Étape 5** Demandez aux utilisateurs d'appuyer sur dièse (#) avant de saisir les chiffres sur l'écran d'activation.

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

**Procédure**

**Étape 1** Appuyez sur **Paramètres**.

**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**.

# Mise à disposition de DNS SRV pour HTTP

La fonctionnalité DNS SRV pour la mise à disposition HTTP active la mise à disposition automatique de votre téléphone multiplateformes. Les enregistrements DNS SRV (Domain Name System Service) établissent des connexions entre un service et un nom d'hôte. Lorsque le téléphone recherche l'emplacement du service de mise à disposition, il commence par interroger le nom de domaine SRV DNS, puis il interroge les enregistrements SRV. Le téléphone valide les enregistrements pour confirmer que le serveur est accessible. Il poursuit ensuite le flux de mise à disposition réel. Les fournisseurs de services peuvent utiliser ce flux de mise à disposition DNS SRV pour assurer la mise à disposition automatique.

DNS SRV base la validation du nom d'hôte sur le certificat du nom de domaine DHCP fourni. Il est important que tous les enregistrements SRV utilisent un certificat valide contenant le nom de domaine DHCP fourni.

La requête DNS SRV inclut le nom de domaine DHCP dans sa construction comme suit : **`_<servicename>._<transport>.<domainName>`**.

Par exemple, **`_ciscoprov-https._tls.example.com`**, indique au téléphone qu'il doit effectuer une recherche pour example.com. Le téléphone utilise le nom d'hôte et le numéro de port récupérés par la requête DNS SRV pour créer l'URL qu'il utilise pour télécharger la configuration initiale.

DNS SRV est l'un des nombreux mécanismes de mise à disposition automatique utilisés par le téléphone. Le téléphone tente les mécanismes dans l'ordre suivant :

1. DHCP
2. SRV DNS
3. EDOS
4. L'activation de périphérique GDS (intégration de code d'activation) ou EDOS

Le tableau ci-dessous décrit les champs de l'enregistrement SRV.

*Tableau 1 : Champs de l'enregistrement SRV*

| Champ | Description | Exemple |
|---|---|---|
| <_servicename.> | Le nom du service commence par un trait de soulignement. Les services de serveur utilisent des noms symboliques dans les enregistrements SRV.<br>Après le service, un point (.) signifie que le service est établi et que la section suivante commence. | **`_ciscoprov-https.`** Ou **`_ciscoprov-http.`**<br>DNS SRV ne prend pas en charge le protocole TFTP. Si vous utilisez TFTP, le message d'erreur suivant s'affiche : `erreur - Le schéma TFTP n'est pas pris en charge dans les recherches SRV.` |
| <_proto.> | Le protocole de transport commence par un trait de soulignement.<br>Le point qui suit le protocole indique que la section du protocole a pris fin. | **`_tls.`** Vous devez utiliser HTTPS avec TLS.<br>ou<br>**`_tcp.`** Vous devez utiliser HTTP avec TCP. |
| <domainName> | Le nom de domaine du service suit le protocole.<br>Validation du nom d'hôte : tous les enregistrements SRV sont validés en fonction du nom de domaine fourni par DHCP. Il est important que tous les enregistrements utilisent un certificat valide contenant le nom de domaine d'origine. | **`example.com`** |
| TTL (Durée de vie) | Valeur d'expiration de l'enregistrement, en secondes. | 86400 |
| Classe | Type d'Internet : notation de liaison standard indiquant qu'il s'agit d'un enregistrement SRV. | IN |
| <priority> | Chaque ligne contient un numéro de priorité. Plus le nombre est faible, plus le téléphone tentera d'essayer le nom d'hôte et le port de l'enregistrement DNS SRV. | **`10`** |
| <weight> | Si deux ou plusieurs services ont la même priorité, le nombre de pondérations détermine la ligne qui a préséance. Plus le nombre est faible, plus le téléphone tentera d'essayer le nom d'hôte et le port de l'enregistrement DNS SRV. | **`20`** |
| <port> | Numéro de port facultatif | **`5060`** |
| <target> | Enregistrement A de la machine fournissant le service.<br>Les enregistrements A sont le type de base de l'enregistrement DNS et sont utilisés pour pointer un domaine ou un sous-domaine vers une adresse IP. | **`pr1.example.com`** |

### Exemples de configurations SRV

_service._proto.name. Port cible de pondération de priorité SRV de la classe TTL.

_ciscoprov-https._tls.example.com. 86400 IN SRV 10 60 5060 pr1.example.com.

_ciscoprov-https._tls.example.com. 86400 10 20 5060 SRV pr2.example.com.

_ciscoprov-http._tcp.example.com. 86400 10 50 5060 SRV px1.example.com.

_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 30 5060 px2.example.com.

## Utiliser DNS SRV pour la mise à disposition HTTP

Les nouveaux téléphones utilisent DNS SRV comme méthode de mise à disposition automatique. Pour les téléphones existants, si votre réseau est configuré pour la mise à disposition à l'aide de DNS SRV pour HTTP, vous pouvez utiliser cette fonction pour resynchroniser votre téléphone. Exemple de fichier de configuration :

```
<flat-profile>
<!-- System Configuration -->
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Profile_Authentication_Type ua="na">Basic Http Authentication </Profile_Authentication_Type>
<Proxy_1_ ua="na">example.com</Proxy_1_>
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>
<User_ID_1_ ua="na">4081001141</User_ID_1_>
</flat-profile>
```

### Avant de commencer

Si vous voulez configurer un serveur de proxy pour le traitement HTTP, assurez-vous de la configuration complète. Reportez-vous à Configurer un serveur de proxy.

### Procédure

Effectuez l'une des actions suivantes : Puis, Définir la règle de profil à l'aide de l'option SRV sur la page Web, à la page 8 ou Définir la règle de profil à l'aide de l'option SRV sur le téléphone, à la page 9

- Placez le fichier de configuration XML, $PSN.xml, dans le `répertoire racine` du serveur Web.
- Placez le fichier de configuration XML, $MA.cfg, dans le `répertoire racine/Cisco/` du serveur Web.

## Définir la règle de profil à l'aide de l'option SRV sur la page Web

Vous pouvez utiliser l'option SRV pour télécharger un fichier de configuration sur votre téléphone.

### Avant de commencer

Accéder à l'interface Web du téléphone

**Procédure**

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

**Étape 2** Dans le champ **Règle de profil**, entrez la règle de profil à l'aide de l'option SRV. Seuls les protocoles HTTP et HTTPS sont pris en charge.

Exemple :

```
[--srv] https://example.com/$PSN.xml
```

## Définir la règle de profil à l'aide de l'option SRV sur le téléphone

Vous pouvez utiliser l'option SRV sur votre téléphone pour télécharger un fichier de configuration.

**Procédure**

**Étape 1** Appuyez sur **Paramètres**.

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

**Étape 3** Entrez la règle de profil à l'aide du paramètre **`[--srv]`**. Seuls les protocoles HTTP et HTTPS sont pris en charge.

Exemple :

```
[--srv] https://example.com/$PSN.xml
```

**Étape 4** Appuyez sur **Resync**.

# 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.

# TR69 RPC Methods

## 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
- Transfert terminé

## 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 :

- Démarrage
- Démarrer
- Modification de valeur
- Demande de connexion
- Périodique
- Transfert terminé
- Télécharger M
- Redémarrer M

# 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 audio 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.

# 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 :

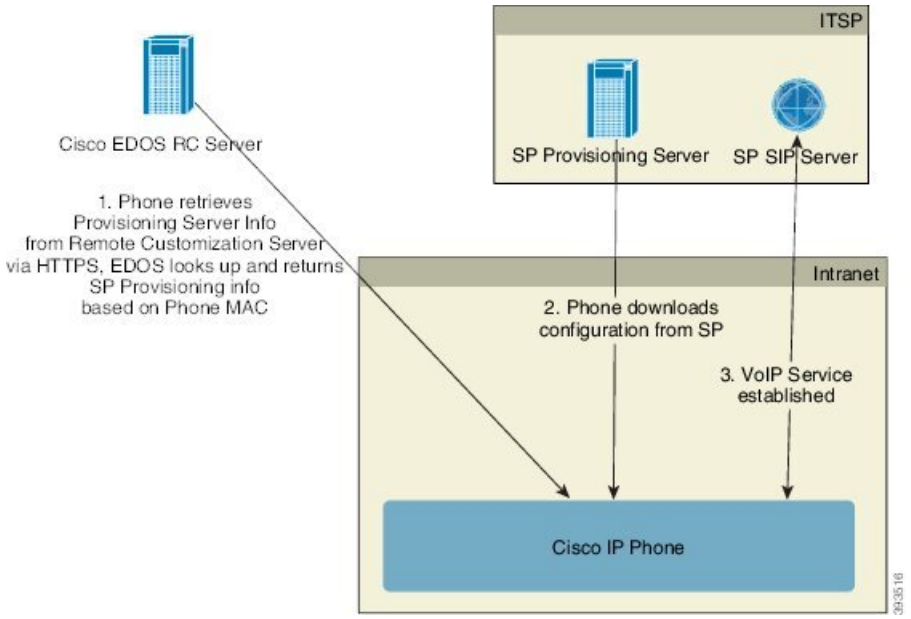
- TFTP (Port UDP 69)
- syslog (Port UDP 514)
- HTTP (TCP port 80)
- HTTPS (Port TCP 443).

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.

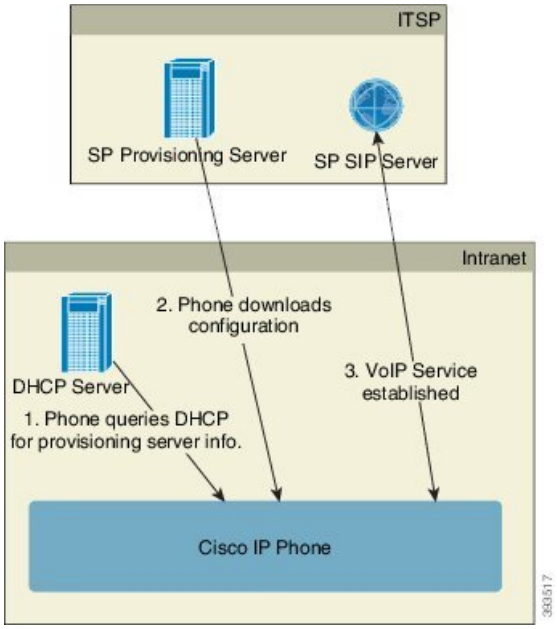
Si le serveur DHCP ne fournit pas d'informations sur le serveur mise à disposition, le téléphone interroge le serveur Cisco EDOS RC et fournit son adresse MAC et modèle, et définit l'état de la personnalisation sur **En attente**. Le serveur Cisco EDOS répond avec les informations du serveur de mise 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 mis 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.

# 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 capable d'obtenir une adresse IP de serveur TFTP directement du serveur DHCP par le biais de l'option 66 du DHCP. Si une Profile_Rule est configurée avec le chemin de fichier de ce serveur TFTP, le périphérique télécharge son profil depuis le serveur TFTP. Le téléchargement se produit lorsque l'appareil est connecté à un réseau local et mis sous tension.

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.

### 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-7832-3PCC :

```
User-Agent: Cisco-CP-7832-3PCC/11.0.1 (00562b043615)
```

L'agent utilisateur est configurable et le téléphone utilise cette valeur s'il n'a pas été configuré (toujours à l'état par défaut).

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 la requête immédiatement avec le nouvel emplacement. |
| **302 Trouvé** | Connu comme déplacé temporairement. | Réessayez la 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 |