Sécurité du téléphone IP Cisco

- Paramétrage de domaine et Internet, à la page 1
- Configuration du test pour les messages SIP INVITE, à la page 4
- Transport Layer Security (Protocole TLS, Sécurité des couches de transport), à la page 5
- Mise à disposition HTTPS, on page 8
- Activer le pare-feu, à la page 11
- Configurer votre pare-feu avec des options supplémentaires, à la page 12
- Configurer la liste de chiffrement, à la page 14
- Activer la vérification du nom d'hôte pour SIP sur TLS, à la page 17
- Activer le mode initié par le client pour les négociations de sécurité du plan des médias, à la page 18
- Authentification 802.1x, à la page 20
- Configurer un serveur proxy, à la page 22
- Configurer une connexion VPN à partir du téléphone, à la page 28
- Configurer une connexion VPN à partir de la page Web du téléphone, à la page 29
- Présentation de la sécurité des produits Cisco, à la page 31

Paramétrage de domaine et Internet

Configuration des domaines d'accès limité

Vous pouvez configurer le téléphone pour qu'il s'enregistre, se mette à disposition, mette à jour le micrologiciel et envoie des rapports à l'aide des serveurs spécifiés. Il n'est pas possible d'effectuer un enregistrement, une mise à disposition, une mise à niveau et un rapport qui n'utilisent pas les serveurs spécifiés sur le téléphone. Si vous spécifiez les serveurs à utiliser, assurez-vous que les serveurs que vous saisissez dans les champs suivants sont inclus dans la liste :

- **Règle de profil**, **Règle de profil B**, **Règle de profil C** et **Règle de profil D** sous l'onglet **Mise à disposition**
- **Règle de mise à niveau** et **Règle de mise à niveau du casque Cisco** sur l'onglet **Mise à disposition**
- **Règle de rapport** sous l'onglet **Mise à disposition**
- **Règle d'autorité de certification personnalisée** sur l'onglet **Mise à disposition**
- **Proxy** et **Proxy sortant** sur l'onglet **Poste(n)**

Avant de commencer

Accéder à l'interface Web du téléphone.

Procédure

Étape 1 Sélectionnez **Voix** > **Système**.

Étape 2 Dans la section **Configuration système**, dans le champ **Domaines d'accès restreint**, saisissez le nom de domaine complets (FQDN) de chaque serveur. Séparez les noms de domaines complets par des virgules.

Exemple :

```
voiceip.com, voiceip1.com
```

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

```
<Restricted_Access_Domains ua="na">voiceip.com, voiceip1.com</Restricted_Access_Domains>
```

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

Configurer les options DHCP

Vous pouvez définir l'ordre dans lequel votre téléphone utilise les options DHCP. Pour obtenir de l'aide sur les options DHCP, reportez-vous à Prise en charge de l'option DHCP, à la page 3.

Avant de commencer

Accéder à l'interface Web du téléphone.

Procédure

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

Étape 2 Dans la section **Profil de configuration**, définissez les paramètres **Option DHCP à utiliser** et **Option DHCPv6 à utiliser** comme décrit dans le tableau Paramètres de configuration des options DHCP, à la page 2.

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

Paramètres de configuration des options DHCP

Le tableau suivant définit la fonction et l'utilisation des paramètres de configuration des options DHCP 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 à l'aide du code XML (cfg.xml) pour configurer un paramètre.

Tableau 1 : Paramètres de configuration des options DHCP

Paramètre	Description
DHCP Option To Use	Options DHCP, délimitées par des virgules, utilisées pour récupérer le micrologiciel et les profils. 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 : `<DHCP_Option_To_Use ua="na">66,160,159,150,60,43,125</DHCP_Option_To_Use>` • Sur la page Web du téléphone, saisissez les options DHCP séparées par des virgules. **Par exemple** : 66,160,159,150,60,43,125 Par défaut : 66,160,159,150,60,43,125
DHCPv6 Option To Use	Options DHCPv6, délimitées par des virgules, utilisées pour récupérer le micrologiciel et les profils. 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 : `<DHCPv6_Option_To_Use ua="na">17,160,159</DHCPv6_Option_To_Use>` • Sur la page Web du téléphone, saisissez les options DHCP séparées par des virgules. **Par exemple** : 17,160,159 Par défaut : 17 160 159

Prise en charge de l'option DHCP

Le tableau suivant énumère les options DHCP prises en charge par les téléphones multiplateformes.

Norme de réseau	Description
DHCP option 1	Masque de sous-réseau
DHCP option 2	Time offset
DHCP option 3	Routeur
DHCP option 6	Serveur de noms de domaine
DHCP option 15	Nom du domaine
DHCP option 41	Durée de bail de l'adresse IP

Norme de réseau	Description
DHCP option 42	Serveur NTP
DHCP option 43	Informations spécifiques au fournisseur Utilisable pour la détection du serveur de configuration automatique TR.69 (ACS)
DHCP option 56	Serveur NTP Configuration du serveur NTP avec IPv6
DHCP option 60	Identifiant de la classe du fournisseur
DHCP option 66	Nom du serveur TFTP
DHCP option 125	Informations spécifiques au fournisseur, qui identifient le fournisseur Utilisable pour la détection du serveur de configuration automatique TR.69 (ACS)
DHCP option 150	Serveur TFTP
DHCP option 159	Adresse IP du serveur de mise à disposition
DHCP option 160	URL de mise à disposition

Configuration du test pour les messages SIP INVITE

Vous pouvez configurer le téléphone pour qu'il teste le message SIP INVITE (initial) lors d'une session. Le test limite les serveurs SIP qui sont autorisés à interagir avec les périphériques du réseau d'un fournisseur de service. Cette pratique empêche les attaques malveillantes contre le téléphone. Si ce paramètre est activé, une autorisation est nécessaire pour les requêtes initiales INVITE entrantes du proxy SIP.

Vous pouvez également configurer les paramètres dans le fichier de configuration du téléphone avec le code XML(cfg.xml).

Avant de commencer

Accéder à l'interface Web du téléphone.

Procédure

Étape 1 Sélectionnez **Voix** > **Poste(n)**, n étant un numéro de poste.

Étape 2 Dans la section **Paramètres SIP**, sélectionnez **Oui** dans la liste **Auto. INVITE** pour activer cette fonction ou cliquez sur **Non** pour la désactiver.

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

```
<Auth_INVITE_1>Yes</Auth_INVITE_1_>
```

Par défaut : **Non**.

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

Transport Layer Security (Protocole TLS, Sécurité des couches de transport)

Le protocole de sécurité des couches de transport (TLS) est un protocole standard permettant de sécuriser et d'authentifier les communications sur Internet. SIP sur TLS chiffre les messages de signalisation SIP entre le proxy SIP du fournisseur de service et l'utilisateur final.

Le téléphone IP Cisco utilise UDP en tant que norme pour le transport SIP, mais il prend aussi en charge SIP sur TLS pour une sécurité renforcée.

Le tableau ci-dessous décrit les deux couches TLS.

Tableau 2 : Couches TLS

Nom du protocole	Description
Protocole d'enregistrement TLS	En couche sur un protocole de transport fiable, tel que SIP ou TCH, il garantit que la connexion est privée à l'aide du cryptage de données symétrique et il assure que la connexion est fiable.
Protocole de négociation TLS	Authentifie le serveur et le client et négocie l'algorithme de cryptage et des clés cryptographiques avant que le protocole d'application ne transmette ou ne reçoive des données.

Chiffrer la signalisation avec SIP sur TLS

Vous pouvez configurer une sécurité renforcée lorsque vous chiffrez les messages de signalisation avec SIP sur TLS.

Avant de commencer

Accéder à l'interface Web du téléphone. Reportez-vous à Transport Layer Security (Protocole TLS, Sécurité des couches de transport), à la page 5

Procédure

Étape 1 Sélectionnez **Voix** > **Poste(n)**, n étant un numéro de poste.

Étape 2 Dans la section **Paramètres SIP**, sélectionnez **TLS** dans la liste **Transport SIP**.

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

```
<SIP_Transport_1_ ua="na">TLS</SIP_Transport_1_>
```

.

Les options disponibles sont :

- UDP
- TCP
- TLS
- Auto

Valeur par défaut : **UDP**

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

Configurer le serveur LDAP sur TLS

Vous pouvez configurer LDAP sur TLS (LDAPS) pour activer la transmission sécurisée des données entre le serveur et un téléphone spécifique.

Attention Cisco recommande de laisser la méthode d'authentification sur la valeur par défaut **Aucune**. En regard du champ Serveur, se trouve un champ d'authentification qui utilise les valeurs **Aucune**, **Simple**, ou **DIGEST-MD5**. Il n'existe pas de valeur **TLS** pour l'authentification. Le logiciel détermine la méthode d'authentification à partir du protocole LDAPS dans la chaîne du serveur.

Vous pouvez également configurer les paramètres dans le fichier de configuration du téléphone avec le code XML(cfg.xml).

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 **LDAP**, saisissez une adresse de serveur dans le champ **Serveur**.

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

```
<LDAP_Server ua="na">ldaps://10.45.76.79</LDAP_Server>
```

Par exemple, saisissez `ldaps://<ldaps_server>[:port]`.

où

- **ldaps://**= le début de la chaîne d'adresse du serveur.
- **ldaps_server** = adresse IP ou nom de domaine
- **port** = numéro de port. Valeur par défaut : 636

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

Configurer StartTLS

Vous pouvez activer le protocole Start Transport Layer Security (StartTLS) pour les communications entre le téléphone et le serveur LDAP. Il utilise le même port réseau (par défaut 389) pour les communications sécurisées et non sécurisées. Si le serveur LDAP prend en charge StartTLS, TLS chiffre les communications. Sinon, les communications sont en texte clair.

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 **LDAP**, saisissez une adresse de serveur dans le champ **Serveur**.

Par exemple, saisissez `ldap://<ldap_server>[:port]`.

Où :

- **`ldaps://`**= le début de la chaîne d'adresse du serveur, schéma de l'URL
- **`ldaps_server`** = adresse IP ou nom de domaine
- **`port`** = numéro de port.

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

```
<LDAP_Server ua="na">ldap://<ldap_server>[:port]</LDAP_Server>
```

Étape 3 Définissez le champ **StartTLS Enable** sur **Oui**.

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

```
<LDAP_StartTLS_Enable ua="na">Oui</LDAP_StartTLS_Enable>
```

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

Sujets connexes

Paramètres de l'annuaire LDAP

Mise à disposition HTTPS

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

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

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

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

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

Obtenir un certificat de serveur signé

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

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

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

Procedure

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

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

Étape 2 Sélectionnez **Gestion des certificats**.

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

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

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

Étape 5 Sélectionnez la méthode de cryptage :

- MD5
- SHA1
- SHA256

Cisco recommande que vous sélectionniez le cryptage SHA256.

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

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

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

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

Étape 9 Cliquez sur **Soumettre**.

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

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

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

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

L'exemple suivant tiré du champ de sujet de certificat client du téléphone IP Cisco 8841 multiplateforme affiche les éléments suivants :

```
OU=CP-8841-3PCC, L=88012BA01234, S=000e08abcdef
```

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

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

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

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

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

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

Serveurs redondants de mise à disposition

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

Syslog Server

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

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

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Activer le pare-feu

Nous avons amélioré la sécurité du téléphone en renforçant le système d'exploitation. Le renforcement de la sécurité garantit que le téléphone dispose d'un pare-feu pour le protéger du trafic entrant malveillant. Le pare-feu surveille les données entrantes et sortantes des ports. Il détecte le trafic entrant provenant de sources inattendues et bloque l'accès. Votre pare-feu autorise tout le trafic sortant.

Le pare-feu peut débloquer dynamiquement les ports normalement bloqués. La connexion TCP sortante ou le flux UDP débloque le port pour le retour et le trafic continu. Le port est maintenu débloqué tant que le flux est actif. Le port passe à l'état Bloqué lorsque le flux est terminé ou périmé.

Les paramètres hérités, Ping de miltidiffusion IPv6**Voix** > **Système** > **Paramètres IPv6** > **Echo de diffusion** continuent de fonctionner indépendamment des nouveaux paramètres du pare-feu.

Les modifications de configuration du pare-feu n'entraînent généralement pas de redémarrage du téléphone. Les redémarrages logiciels du téléphone ne modifient généralement pas le fonctionnement du pare-feu.

Le pare-feu est activé par défaut. S'il est désactivé, vous pouvez l'activer à partir de la page Web du téléphone.

Avant de commencer

Accéder à l'interface Web du téléphone

Procédure

Étape 1 sélectionnez **Voix** > **Système** > **Paramètres de sécurité**.

Étape 2 Dans la liste déroulante **Pare-feu**, sélectionnez **Activé**.

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

```
<Firewall ua="na">Enabled</Firewall>
```

Les valeurs autorisées sont Désactivé | Activé. La valeur par défaut est Activé.

Étape 3 Cliquez sur **Envoyer toutes les modifications**.
Cela active le pare-feu avec ses ports UDP et TCP ouverts par défaut.

Étape 4 Sélectionnez **Désactivé** pour désactiver le pare-feu si vous souhaitez que votre réseau repasse à son comportement précédent.

Le tableau suivant décrit les différents ports UDP ouverts :

Tableau 3 : Ports UDP ouverts par défaut du pare-feu

Port UDP ouvert par défaut	Description
DHCP/DHCPv6	Port du client DHCP 68 Port du client DHCPv6 546
SIP/UDP	Configurez le port dans **Voice** > **Ext<n>** > **SIP Settings** > **SIP Port** (exemple : 5060), lorsque **Line Enable** est réglé sur **`Yes`**, et **SIP Transport** est réglé sur **`UDP`** ou **`Auto`**.
Protocoles RTP/RTCP	Plage de ports UDP comprise entre **`Port RTP Min`** et **`Port RTP Max+1`**
PFS (Peer Firmware Sharing, Partage de micro-programme avec les homologues)	Le port 4051, **lorsque l'** activation **de la mise** à niveau et **`le partage du micrologiciel d'homologue sont définis sur Oui`**.
Clien TFTP	Ports 53240-53245. Vous avez besoin de cette plage de ports si le serveur distant utilise un port autre que le port standard TFTP 69. Vous pouvez la désactiver si le serveur utilise le port standard 69. Voir Configurer votre pare-feu avec des options supplémentaires, à la page 12.
TR-069	Le port UDP/STUN 7999, lorsque **Activer TR-069** est défini sur **`Oui`**.

Le tableau suivant décrit les différents ports TCP ouverts :

Tableau 4 : Ports TCP ouverts par défaut du pare-feu

Port TCP ouvert par défaut	Description
Serveur Web	Port configuré via le port du serveur Web (par défaut 80), lorsque**Activer le serveur Web** est défini sur **`Oui`**.
PFS (Peer Firmware Sharing, Partage de micro-programme avec les homologues)	Les ports 4051 et 6970, lorsque **Activation de la mise à niveau** et **Partage de micrologiciel par les homologues**, sont tous deux définis sur **`Oui`**.
TR-069	Le port HTTP/SOAP de l'URL de demande de connexion TR-069, lorsque **Activer TR-069** est défini sur **`Oui`**. Le port est choisi de manière aléatoire dans la plage 8000-9999.

Configurer votre pare-feu avec des options supplémentaires

Vous pouvez configurer des options supplémentaires dans le champ **Options du pare-feu**. Saisissez le mot-clé de chaque option du champ et séparez les mots-clés par des virgules (,). Certains mots clés comportent des valeurs. Séparez les valeurs par des deux-points (:).

Avant de commencer

Accéder à l'interface Web du téléphone

Procédure

Étape 1 Allez dans **Voix** > **Système** > **Paramètres de sécurité**.

Étape 2 Sélectionnez **Activé** pour le champ **Pare-feu**.

Étape 3 Dans le champ **Options dde pare-feu**, saisissez les mots-clés. La liste des ports s'applique aux protocoles IPv4 et IPv6.

Lorsque vous saisissez les mots-clés,

- séparez les mots-clés par des virgules (,).
- séparez les valeurs des mots-clés par des deux-points (:).

Tableau 5 : Paramètres facultatifs du pare-feu

Mots clés des options de pare-feu	Description
Le champ est vide.	Le pare-feu s'exécute avec les ports ouverts par défaut.
NO_ICMP_PING	Le pare-feu bloque les demandes **d'écho** ICMP/ICMPv6 entrantes (ping). Cette option peut empêcher certains types de requêtes traceroute vers le téléphone. Windows **tracert** est un exemple. Exemple de saisie **d'options de pare-feu** avec une combinaison d'options : NO_ICMP_PING,TCP:12000,UDP:8000:8010 Le pare-feu s'exécute avec les paramètres par défaut et les options supplémentaires suivantes : • Supprime les demandes **d'écho** ICMP/ICMPv6 entrantes. • Ouvre le port TCP 12000 (IPv4 et IPv6) pour les connexions entrantes. • Ouvre la plage de ports UDP 8000 à 8010 (IPv4 et IPv6) pour les demandes entrantes.
NO_ICMP_UNREACHABLE	Le téléphone n'envoie pas de `destination ICMP/ICMPv6 inaccessible` pour les ports UDP. **Remarque** La seule exception est de toujours envoyer `Destination inaccessible` pour les ports de la plage de ports RTP. Cette option peut empêcher certains types de requêtes **traceroute** vers le périphérique. Par exemple, Linux **traceroute** peut être rompue.

Mots clés des options de pare-feu	Description
NO_CISCO_TFTP	• Le téléphone n'ouvre pas la plage de ports TCP client (UDP 53240:53245). • Les demandes adressées à des ports de serveur TFTP non standard (non 69) échouent. • Les demandes adressées au port de serveur TFTP standard 69 réussissent.
Les mots clés et options suivants s'appliquent lorsque le téléphone exécute des applications personnalisées qui traitent les demandes entrantes.	
UDP :<xxx>	Ouvre le port TCP <xxx>.
UDP :<xxx:yyy>	Ouvre la plage de ports UDP,<xxx to yyy> , inclusivement. Vous pouvez avoir jusqu'à 5 options de port UDP (ports uniques et plages de ports). Par exemple, vous pouvez avoir 3 UDP :<xxx> et 2 UDP :<xxx:yyy>.
TCP :<xxx>	Ouvre le port TCP <xxx>.
TCP :<xxx:yyy>	Ouvre la plage de ports TCP <xxx to yyy>, inclusivement. Vous pouvez avoir jusqu'à 5 options de port TCP (ports uniques et plages de ports). Par exemple, vous pouvez avoir 4 TCP :<xxx> et un TCP :<xxx:yyy>.

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

```
<Firewall_Config ua="na">NO_ICMP_PING</Firewall_Config>
```

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

Configurer la liste de chiffrement

Vous pouvez spécifier les suites de chiffrement que les applications TLS du téléphone utilisent. La liste de chiffrement spécifiée s'applique à toutes les applications qui utilisent le protocole TLS. Les applications TLS de votre téléphone sont les suivantes :

- Mise à disposition de l'autorité de certification du client
- Géolocalisation E911
- Mise à niveau du micrologiciel/du casque Cisco

- LDAPS
- LDAP (StartTLS)
- Téléchargement d'image
- Téléchargement de ogo
- Téléchargement du dictionnaire
- Mise à disposition
- Téléchargement d'un rapport
- Chargement PRT
- SIP sur TLS
- TR-069
- API Websocket
- Services XML
- Services XSI

Vous pouvez également spécifier les suites de chiffrement à l'aide du paramètre `TDevice.X_CISCO_SecuritySettings.TLSCipherList` ou du fichier de configuration (cfg.xml). Dans le fichier de configuration du téléphone, entrez une chaîne au format suivant :

```
<TLS_Cipher_List ua="na">RSA:!aNULL:!eNULL</TLS_Cipher_List>
```

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** > **Système**.

Étape 2 Dans la section **Paramètres de sécurité**, entrez la suite de chiffrement ou la combinaison de suites de chiffrement dans le champ **Liste de chiffrement TLS**.

Par exemple :

```
RSA:!aNULL:!eNULL
```

Prend en charge ces suites de chiffrement à l'aide de l'authentification RSA, mais exclut les suites de chiffrement n'offrant aucun chiffrement ni authentification.

Remarque Une liste de chiffrement valide doit respecter le format défini à https://www.openssl.org/docs/man1.1.1/man1/ciphers.html. Votre téléphone ne prend pas en charge toutes les chaînes de chiffrement répertoriées dans la page Web OpenSSL. Pour les chaînes prises en charge, reportez-vous à Chaînes de chiffrement prises en charge, à la page 16.

Si la valeur du champ **Liste de chiffrement TLS** est vide ou non valide, les suites de chiffrement utilisées varient selon les applications. Reportez-vous à la liste suivante pour les suites que les applications utilisent lorsque ce champ comporte une valeur vide ou incorrecte.

- Les applications de serveur Web (HTTPS) utilisent les suites de chiffrement suivantes :
  - **ECDHE-RSA-AES256-GCM-SHA384**
  - **ECDHE-RSA-AES128-GCM-SHA256**
  - **AES256-SHA**
  - **AES128-SHA**
  - **DES-CBC3-SHA**
- XMPP utilise la liste de chiffrement **HIGH:MEDIUM:AES:@STRENGTH**.
- SIP, TR-069, ainsi que d'autres applications utilisant la bibliothèque curl utilisent la chaîne de chiffrement **PAR DÉFAUT**. La chaîne de chiffrement **PAR DÉFAUT** contient les suites de chiffrement suivantes prises en charge par le téléphone :

```
DEFAULT Cipher Suites (28 suites):
        ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ECDHE_RSA_WITH_AES_256_GCM_SHA384
        DHE_RSA_WITH_AES_256_GCM_SHA384
        ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        ECDHE_RSA_WITH_AES_128_GCM_SHA256
        DHE_RSA_WITH_AES_128_GCM_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        ECDHE_RSA_WITH_AES_256_CBC_SHA384
        DHE_RSA_WITH_AES_256_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        ECDHE_RSA_WITH_AES_128_CBC_SHA256
        DHE_RSA_WITH_AES_128_CBC_SHA256
        ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        ECDHE_RSA_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
        ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        ECDHE_RSA_WITH_AES_128_CBC_SHA
        DHE_RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_GCM_SHA384
        RSA_WITH_AES_128_GCM_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA
        EMPTY_RENEGOTIATION_INFO_SCSV
```

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

Chaînes de chiffrement prises en charge

Les chaînes de chiffrement prises en charge répertoriées ci-dessous sont basées sur les normes OpenSSL 1.1.1d.

Tableau 6 : Chaînes de chiffrement prises en charge (OpenSSL 1.1.1d)

Chaînes	Chaînes	Chaînes
DÉFAUT	kECDHE, kEECDH	CAMELLIA128, CAMELLIA256, CAMELLIA
COMPLEMENTOFDEFAULT	ECDHE, EECDH	CHACHA20
TOUT	Les	SEED
COMPLEMENTOFALL	AECDH	MD5
ÉLEVÉ	aRSA	SHA1, SHA
MOYEN	aDSS, DSS	SHA256, SHA384
eNULL NULL	aECDSA, ECDSA	SUITEB128, SUITEB128ONLY, SUITEB192
aNULL	TLSv 1.2, TLSv1, SSLv3	
kRSA, RSA	AES128, AES256, AES	
kDHE, kEDH, DH	AESGCM	
DHE, EDH	AESCCM, AESCCM8	
ADH	ARIA128, ARIA256, ARIA	

Activer la vérification du nom d'hôte pour SIP sur TLS

Vous pouvez activer la sécurité améliorée du téléphone sur une ligne téléphonique si vous utilisez TLS. La ligne téléphonique peut vérifier le nom d'hôte pour déterminer si la connexion est sécurisée.

Sur une connexion TLS, le téléphone peut vérifier le nom d'hôte pour vérifier l'identité du serveur. Le téléphone peut vérifier à la fois l'autre nom du sujet (SAN) et le nom commun de du sujet (CN). Si le nom d'hôte du certificat valide correspond au nom d'hôte utilisé pour communiquer avec le serveur, la connexion TLS est établie. Sinon, la connexion TLS échoue.

Le téléphone vérifie toujours le nom d'hôte pour les applications suivantes :

- LDAPS
- LDAP (StartTLS)
- XMPP
- Mise à niveau de l'image via HTTPS
- XSI sur HTTPS
- Téléchargement de fichier via HTTPS
- TR-069

Lorsqu'une ligne téléphonique transporte des messages SIP sur TLS, vous pouvez configurer la ligne pour activer ou ignorer la vérification du nom d'hôte à l'aide du champ **Valider le nom TLS** de l'onglet **Poste(n)**.

Avant de commencer

- Accéder à la page Web d'administration du téléphone. Reportez-vous à Accéder à l'interface Web du téléphone.
- Sur l'onglet **Poste(n)**, définissez le **Transport SIP** sur **TLS**.

Procédure

Étape 1 Allez à **Voix** > **Poste(n)**.

Étape 2 Dans la section **Proxy et enregistrement** , configurez le champ **Valider le nom TLS** sur **Oui** pour activer la vérification de l' hôte ou sur **Non** pour ignorer la vérification de l'hôte.

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

```
<TLS_Name_Validate_1_ ua="na">Yes</TLS_Name_Validate_1_>
```

Les valeurs autorisées sont Oui ou Non. Le paramètre par défaut est Oui.

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

Activer le mode initié par le client pour les négociations de sécurité du plan des médias

Pour protéger les sessions multimédias, vous pouvez configurer le téléphone pour qu'il initie les négociations de sécurité du plan de support avec le serveur. Le mécanisme de sécurité suit les normes énoncées dans le document RFC 3329 et son projet d'extension *Noms du mécanisme de sécurité pour les médias* (reportez-vous à https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2). Le transport des négociations entre le téléphone et le serveur peut utiliser le protocole SIP sur UDP, TCP et TLS. Vous pouvez limiter la négociation de la sécurité du plan de support pour qu'elle ne s'applique que lorsque le protocole de transport de signalisation est TLS.

Vous pouvez également configurer ces paramètres dans le fichier de configuration du téléphone (cfg.xml). Pour configurer chaque paramètre, reportez-vous à la syntaxe de la chaîne dans Paramètres de la négociation de sécurité du plan de support, à la page 19.

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** > **Poste(n)**.

Étape 2 Dans la section **Paramètres SIP**, définissez le champ **Demande de MediaSec** et **MediaSec sur TLS uniquement**, comme défini dans Paramètres de la négociation de sécurité du plan de support, à la page 19

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

Paramètres de la négociation de sécurité du plan de support

Le tableau ci-dessous définit la fonction et l'utilisation des paramètres de la négociation de la sécurité du olan de support dans la section **Paramètres SIP** sous l'onglet **Voix**> **Poste(n)** 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 7 : Paramètres de la négociation de sécurité du plan de support

Paramètre	Description
Demande MediaSec	Indique si le téléphone initie des négociations de sécurité du plan de support avec le serveur. 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 : `<MediaSec_Request_1_ ua="na">Yes</MediaSec_Request_1_>` • Dans l'interface Web du téléphone, définissez ce champ sur **Oui** ou **Non** en fonction des besoins. Valeurs autorisées : Oui | Non • **Oui** : mode initié par le client. Le téléphone initie des négociations de sécurité du plan de support. • **Non** : mode initié par le serveur. Le serveur initie des négociations de sécurité du plan de support. Le téléphone n'initie pas de négociations, mais peut traiter les demandes de négociation provenant du serveur pour établir des appels sécurisés. Par défaut : Non

Paramètre	Description
MediaSec sur TLS uniquement	Spécifie le protocole de transport de signalisation sur lequel la négociation de sécurité du plan de média est appliquée. Avant de définir ce champ sur **Oui**, assurez-vous que le protocole de transport de signalisation est TLS. 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 : `<MediaSec_Over_TLS_Only_1_ ua="na">No</MediaSec_Over_TLS_Only_1_>` • Dans l'interface Web du téléphone, définissez ce champ sur **Oui** ou **Non** en fonction des besoins. Valeurs autorisées : Oui | Non • **Oui** : le téléphone initie ou traite les négociations de sécurité du plan de support uniquement lorsque le protocole de transport de signalisation est TLS. • **Non** : le téléphone initie et traite les négociations de sécurité du plan de support indépendamment du protocole de transport de signalisation. Par défaut : Non

Authentification 802.1x

Les téléphones IP Cisco utilisent le protocole de découverte Cisco (CDP) pour identifier le commutateur LAN et déterminer les paramètres tels que l'allocation VLAN et les besoins en alimentation en ligne. CDP n'identifie pas localement les postes de travail raccordés. Les téléphones IP Cisco fournissent un mécanisme de connexion directe à EAPOL. Grâce à ce mécanisme, un poste de travail raccordé au téléphone IP Cisco peut faire passer des messages EAPOL à l'authentifiant 802.1X et au commutateur LAN. Le mécanisme de connexion directe assure que le téléphone IP n'agisse pas en tant que commutateur LAN pour authentifier un terminal de données avant d'accéder au réseau.

Les téléphones IP Cisco fournissent également un mécanisme de déconnexion d'EAPOL par proxy. Si l'ordinateur raccordé localement est déconnecté du téléphone IP, le commutateur LAN ne détecte pas l'interruption de la liaison physique, car la liaison entre le commutateur LAN et le téléphone IP est maintenue. Pour éviter de compromettre l'intégrité du réseau, le téléphone IP envoie au commutateur un message EAPOL-Logoff au nom de l'ordinateur en aval, pour que le commutateur LAN efface la valeur d'authentification correspondant à l'ordinateur en aval.

La prise en charge de l'authentification 802.1X requiert plusieurs composants :

- Téléphone IP Cisco : le téléphone envoie la requête d'accès au réseau. Les téléphones IP Cisco contiennent un demandeur 802.1X. Ce demandeur permet aux autoriser de contrôler la connectivité des téléphones IP aux ports de commutation LAN. La version actuelle du demandeur 802.1X du téléphone utilise les options EAP-FAST et EAP-TLS pour l'authentification réseau.

- Cisco Secure Access Control Server (ACS) (ou un autre serveur d'authentification tiers) : le serveur d'authentification et le téléphone doivent tous deux être configurés avec un secret partagé qui authentifie le téléphone.
- Un commutateur LAN prenant en charge la norme 802.1X : le commutateur agit comme authentifiant et transmet les messages entre le téléphone et le serveur d'authentification. Une fois l'échange terminé, le commutateur accorde ou refuse au téléphone l'autorisation d'accéder au réseau.

Vous devez effectuer les actions suivantes pour configurer 802.1X.

- Configurez les autres composants avant d'activer l'authentification 802.1X sur le téléphone.
- Configure PC Port (Configurer le port PC) : La norme 802.1X ne tenant pas compte des VLAN, il est recommandé qu'un seul périphérique soit authentifié pour un port de commutation donné. Toutefois, certains commutateurs prennent en charge l'authentification sur plusieurs domaines. La configuration du commutateur détermine si vous pouvez brancher un ordinateur dans le port PC du téléphone.
  - Oui : si vous utilisez un commutateur qui prend en charge l'authentification sur plusieurs domaines, vous pouvez activer le port PC et y brancher un ordinateur. Dans ce cas, les téléphones IP Cisco prennent en charge la déconnexion d'EAPOL par proxy pour surveiller les échanges d'authentification entre le commutateur et l'ordinateur relié.
  - Non : si le commutateur ne prend pas en charge plusieurs périphériques compatibles 802.1X sur le même port, vous devez désactiver le port PC lorsque l'authentification 802.1X est activée. Si vous ne désactivez pas ce port et tentez par la suite d'y raccorder un ordinateur, le commutateur refusera l'accès réseau au téléphone et à l'ordinateur.
- Configure Voice VLAN (Configurer le VLAN voix) : la norme 802.1X ne tenant pas compte des VLAN, vous devez configurer ce paramètre en fonction de la prise en charge du commutateur.
  - Activé : si vous utilisez un commutateur qui prend en charge l'authentification sur plusieurs domaines, vous pouvez continuer à utiliser le VLAN voix.
  - Désactivé : si le commutateur ne prend pas en charge l'authentification sur plusieurs domaines, désactivez le VLAN voix et envisagez d'affecter le port à un VLAN natif.

Enable 802.1X Authentication

Vous pouvez activer l'authentification 802.1X sur le téléphone Lorsque l'authentification 802.1X est activée, le téléphone utilise l'authentification 802.1X pour demander l'accès au réseau. Lorsque l'authentification 802.1X est désactivée, le téléphone utilise CDP pour obtenir l'accès au VLAN et au réseau. Vous pouvez également afficher l'état de la transaction dans le menu de l'écran du téléphone.

Procédure

Étape 1 Effectuez l'une des actions suivantes pour activer l'authentification 802.1 X :

- Dans l'interface Web du téléphone, sélectionnez **Voix** > **Système** et définissez le champ **Activer l'authentification 802.1X** sur **Oui**. Cliquez ensuite sur **Envoyer toutes les modifications**.
- Dans le fichier de configuration du téléphone (cfg.xml), entrez une chaîne au format suivant :

```
<Enable_802.1X_Authentication ua="rw">Yes</Enable_802.1X_Authentication>
```

- Sur le téléphone, appuyez sur **Application** > **Configuration réseau** > **Configuration Ethernet** > **Authentification 802.1X**. Basculez ensuite le champ **Authentification du périphérique** sur **Activé** à l'aide du bouton **Sélectionner** puis appuyer sur **Envoyer**.

Étape 2 (Facultatif) Sélectionnez **État de la transaction** pour afficher les informations suivantes :

- **État de la transaction** : affiche l'état de l'authentification 802.1x : L'État peut être
  - *En cours d'authentifiaction* : indique que le processus d'authentification est en cours.
  - *Authentifié* : indique que le téléphone est authentifié.
  - *Désactivé* : indique que l'authentification 802.1 x est désactivée sur le téléphone.
- **Protocole** : affiche la méthode EAP utilisée pour l'Authentification 802.1x Il peut s'agir du protocole EAP-FAST ou EAP-TLS.

Étape 3 Appuyez sur pour quitter le menu.

Configurer un serveur proxy

Vous pouvez configurer le téléphone pour qu'il utilise un serveur proxy afin de renforcer la sécurité. Un serveur proxy agit comme un pare-feu entre le téléphone et Internet. Après une configuration réussie, le téléphone se connecte à Internet par le biais du serveur proxy, ce qui le protège des cyberattaques.

Vous pouvez configurer un serveur proxy en utilisant un script de configuration automatique ou en configurant manuellement le serveur hôte (nom d'hôte ou adresse IP) et le port du serveur proxy.

Une fois configurée, la fonction de proxy HTTP s'applique à toutes les applications qui utilisent le protocole HTTP. Les applications comprennent les suivantes :

- GDS (Embarquement du code d'activation)
- Activation du périphérique EDOS
- Intégration à Webex Cloud (via EDOS et GDS)
- Certificat d'authentification
- Mise à disposition
- Mise à niveau du micrologiciel
- Rapport d'état du téléphone
- Chargement PRT
- Services XSI
- Services Webex

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** > **Système**.

Étape 2 Dans la section **HTTP Proxy Settings**, configurez le paramètre **Proxy Mode** et d'autres paramètres en fonction de vos besoins. Les procédures détaillées sont fournies dans les étapes suivantes.

Étape 3 Effectuez l'une des actions suivantes :

- **Le mode Proxy** est **Auto** :
  - Si la valeur de **Use Auto Discovery (WPAD)** est **Oui**, aucune autre action n'est requise. Le téléphone récupère automatiquement un fichier PAC (Proxy Auto-Configuration) par le protocole WPAD (Web Proxy Auto-Discovery).
  - Si **Use Auto Discovery (WPAD)** est **Non**, entrez une URL valide dans **PAC URL**.
- **Le mode Proxy** est **Manuel** :
  - Si **Proxy Server Requires Authentication** est **Non**, entrez un serveur proxy dans **Proxy Host** et un port proxy dans **Proxy Port**.
  - Si **Proxy Server Requires Authentication** est **Yes**, entrez un serveur **proxy dans Proxy Host** et un port proxy dans **Proxy Port**. Et saisissez un nom d'utilisateur dans **Nom d'utilisateur** et un mot de passe dans **Mot de passe**.
- **Si le mode Proxy** est **désactivé**, la fonction proxy HTTP est désactivée sur le téléphone.

Vous pouvez également configurer ces paramètres dans le fichier de configuration du téléphone (cfg.xml). Pour configurer chaque paramètre, reportez-vous à la syntaxe de la chaîne dans la section Paramètres du proxy HTTP, à la page 23.

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

Paramètres du proxy HTTP

Le tableau suivant définit la fonction et l'utilisation des paramètres du proxy HTTP dans la section **Paramètres du proxy HTTP** sous l'onglet **Système** > **vocal** dans 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 8 : Paramètres du proxy HTTP

Paramètre	Description et valeur par défaut
Mode proxy	Spécifie le mode proxy HTTP utilisé par le téléphone, ou désactive la fonctionnalité Proxy HTTP. • Auto Le téléphone récupère automatiquement un fichier PAC (Proxy Auto-Configuration) pour sélectionner un serveur proxy. Dans ce mode, vous pouvez déterminer s'il faut utiliser le protocole Web Proxy Auto-Discovery (WPAD) pour récupérer un fichier PAC ou entrer manuellement une URL valide du fichier. Pour plus de détails sur les paramètres, voir Utiliser la découverte automatique (WPAD) et l'URL du PAC. • Manuelle Vous devez spécifier manuellement un serveur (nom d'hôte ou adresse IP) et un port d'un serveur proxy. Pour plus de détails sur les paramètres, voir Hôte du proxy et Port du proxy. • Désactivé Vous désactivez la fonction de proxy HTTP sur le téléphone. 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 : `<Proxy_Mode ua="rw">Off</Proxy_Mode>` • Sur l'interface Web du téléphone, sélectionnez un mode proxy ou désactivez la fonction. Valeurs autorisées : Auto, Manuel, et Désactivé Par défaut : Désactivé

Paramètre	Description et valeur par défaut
Utiliser la détection automatique (WPAD)	Détermine si le téléphone utilise le protocole Web Proxy Auto-Discovery (WPAD) pour récupérer un fichier PAC. Le protocole WPAD utilise DHCP ou DNS, ou les deux protocoles réseau pour localiser automatiquement un fichier PAC (Proxy Auto-Configuration). Le fichier PAC est utilisé pour sélectionner un serveur proxy pour une URL donnée. Ce fichier peut être hébergé localement ou sur un réseau. • La configuration du paramètre prend effet lorsque le **mode Proxy** est défini sur **Auto**. • Si vous définissez le paramètre sur **Non**, vous devez spécifier une URL PAC. Pour plus de détails sur ce paramètre, voir URL PAC. 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 : `<Use_Auto_Discovery__WPAD_ ua="rw">Yes</Use_Auto_Discovery__WPAD_>` • Sur l'interface Web du téléphone, sélectionnez Oui ou Non selon le cas. Valeurs autorisées : Oui et Non. Par défaut : Oui
URL PAC	URL d'un fichier PAC. Par exemple, `http://proxy.department.branch.example.com` TFTP, HTTP et HTTPS sont pris en charge. Si vous réglez le **Mode Proxy** sur **Auto** et l'option **Utiliser la découverte automatique (WPAD)** sur **Non**, vous devez configurer ce paramètre. 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 : `<PAC_URL ua="rw">http://proxy.department.branch.example.com/pac</PAC_URL>` • Sur l'interface Web du téléphone, entrez une URL valide qui permet de localiser un fichier PAC. Valeur par défaut : vide

Paramètre	Description et valeur par défaut

Hôte proxy	Adresse IP ou nom d'hôte du serveur hôte proxy auquel le téléphone doit accéder. Par exemple :
	`proxy.example.com`
	Le schéma (`http://` or `https://`) n'est pas requis.
	Si vous définissez le **mode Proxy** sur **Manuel**, vous devez configurer ce paramètre.
	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 :
	`<Proxy_Host ua="rw">proxy.example.com</Proxy_Host>`
	• Sur l'interface Web du téléphone, entrez l'adresse IP ou le nom d'hôte du serveur proxy.
	Valeur par défaut : vide

Port proxy	Numéro de port du serveur hôte proxy. Si vous définissez le **mode Proxy** sur **Manuel**, vous devez configurer ce paramètre. 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 : `<Proxy_Port ua="rw">3128</Proxy_Port>` • Sur l'interface Web du téléphone, entrez un port de serveur. Par défaut : 3128

Paramètre	Description et valeur par défaut
Le serveur proxy nécessite une authentification	Détermine si l'utilisateur doit fournir les informations d'identification (nom d'utilisateur et mot de passe) requises par le serveur proxy. Ce paramètre est configuré selon le comportement actuel du serveur proxy. Si vous définissez ce paramètre sur **Oui**, vous devez configurer **Nom d'utilisateur** et **Mot de passe**. Pour plus de détails sur les paramètres, voir Nom d'utilisateur et Mot de passe. La configuration du paramètre prend effet lorsque le **mode Proxy** est défini sur **Manuel**. 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 : `<Proxy_Server_Requires_Authentication ua="rw">No</Proxy_Server_Requires_Authentication>` • Sur l'interface Web du téléphone, définissez ce champ sur Oui ou Non en fonction des besoins. Valeurs autorisées : Oui et Non. Par défaut : Non
Nom d'utilisateur	Nom d'utilisateur pour un utilisateur d'identifiant sur le serveur proxy. Si **Mode Proxy** est défini sur **Manuel** et **Serveur Proxy exigeant une authentification** est défini sur **Oui**, vous devez configurer le paramètre. 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 : `<Proxy_Username ua="rw">Example</Proxy_Username>` • Sur l'interface Web du téléphone, saisissez le nom d'utilisateur. Valeur par défaut : vide
Mot de passe	Mot de passe du nom d'utilisateur spécifié à des fins d'authentification sur le serveur proxy. Si le **mode Proxy** est défini sur **Manuel** et si le paramètre **Serveur Proxy exige une authentification** est défini sur **Oui**, vous devez configurer ce paramètre. 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 : `<Proxy_Password ua="rw">Example</Proxy_Password>` • Sur l'interface Web du téléphone, saisissez un mot de passe valide pour l'authentification proxy de l'utilisateur. Valeur par défaut : vide

Configurer une connexion VPN à partir du téléphone

Vous pouvez configurer et activer la connexion VPN à partir du téléphone.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionnez **Configuration de réseau** > **Paramètres VPN**.

Étape 3 Saisissez l'adresse IP ou le nom de domaine complet d'un serveur VPN dans **VPN serveur**.

Étape 4 Saisissez les informations d'authentification de l'utilisateur dans **Nom d'utilisateur** et **Mot de passe**.

Étape 5 (Facultatif) Au besoin, saisissez le nom d'un groupe de tunnels dans **Groupe de tunnels**.

Si le champ est vide, cela signifie qu'aucun groupe de tunnels n'est utilisé pour cette connexion VPN.

Étape 6 Mettez en surbrillance **connexion au VPN au démarrage**, appuyez sur le bouton **Sélectionner** du cluster de navigation pour sélectionner **Activé** .

Étape 7 Appuyez sur **Définir** pour enregistrer les paramètres.

Actuellement, les paramètres VPN sont terminés. Vous pouvez redémarrer manuellement le téléphone pour déclencher la connexion automatique au serveur VPN. Si vous voulez activer la connexion VPN immédiatement, passez à l'étape suivante.

Étape 8 Mettez en surbrillance **Activer la connexion** VPN, sélectionnez **On** pour activer la connexion VPN.

Remarque Lorsque vous réglez l'option **Activer la connexion VPN** sur **Activé**, le téléphone tente immédiatement de se connecter au serveur VPN. Durant le processus, le téléphone redémarre automatiquement.

La connexion VPN prend environ une minute.

Après le redémarrage du téléphone, l'icône de connexion VPN dans le coin supérieur droit de l'écran du téléphone indique que la connexion VPN est établie avec succès.

Si la connexion VPN échoue, la valeur **Activer la connexion VPN** reste **Désactivé**.

Étape 9 (Facultatif) Afficher les détails de la connexion VPN. Par exemple, l'état actuel de la connexion VPN et l'adresse IP du VPN. Pour plus d'informations, reportez-vous à Affichage de l'état du VPN, à la page 29.

Étape 10 (Facultatif) Vous pouvez désactiver la connexion VPN à partir du téléphone.

a) Appuyez sur **Applications** .
b) Sélectionnez **Configuration de réseau** > **Paramètres VPN**.
c) Mettez en surbrillance **Connecter au VPN au démarrage**, sélectionnez **Désactivé**.
d) Mettez en surbrillance **Activer la connexion VPN**, sélectionnez **Désactiver** pour désactiver la connexion VPN. Cela entraîne un redémarrage immédiat du téléphone.

Affichage de l'état du VPN

Vous pouvez vérifier les détails de la connexion VPN. Par exemple, l'état actuel du VPN et l'adresse IP du VPN de votre téléphone.

Vous pouvez également afficher le statut à partir de la page Web du téléphone en sélectionnant **Info** > **Statut** > **Statut du VPN**.

Procédure

Étape 1 Appuyez sur **Applications** .

Étape 2 Sélectionner **Statut** > **Statut du VPN**.

Vous pouvez afficher les informations suivantes :

- **connexion VPN :** indique si le téléphone se connecte au serveur VPN. L'État peut être `Connecté` ou `Déconnecté`.
- **VPN adresse IP :** adresse IP VPN attribuée par le serveur VPN.
- **VPN masque de sous-réseau :** masque de sous-réseau VPN attribué par le serveur VPN.
- **octets envoyés :** nombre total d'octets envoyés par le téléphone au réseau via le serveur VPN.
- **octets reçus :** nombre total d'octets reçus depuis le réseau via le serveur VPN.

Configurer une connexion VPN à partir de la page Web du téléphone

Vous pouvez configurer une connexion VPN à partir de la page Web 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** > **Système**.

Étape 2 Dans la section **Paramètres VPN**, configurez les paramètres comme définis dans le tableau Paramètres VPN, à la page 30.

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

Les changements ne prennent pas effet immédiatement. Vous devez redémarrer manuellement le téléphone ou activer la connexion VPN à partir du téléphone pour déclencher la connexion VPN.

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 le tableau Paramètres VPN, à la page 30.

Étape 4 (Facultatif) Une fois que le téléphone a redémarré avec succès, vous pouvez afficher le statut et d'autres détails de la connexion VPN dans la section **VPN Status** de**Info** > **Status**.

Étape 5 (Facultatif) Si vous voulez désactiver la connexion VPN, réglez le paramètre **Connecter au démarrage** sur **Non**, puis redémarrez manuellement le téléphone. Pour plus d'informations, reportez-vous à Redémarrer le téléphone à partir de la page Web du téléphone.

Paramètres VPN

Le tableau suivant définit la fonction et l'utilisation des paramètres de connexion VPN dans la section **Paramètres VPN** sous l'onglet**Système** > **vocal**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 9 : Paramètres VPN

Paramètre	Description et valeur par défaut

Serveur VPN	Adresse IP ou FQDN du serveur VPN auquel le téléphone doit accéder. Par exemple :
	`100.101.1.218` ou `vpn_server.example.com`
	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 :
	`<VPN_Server ua="rw"><Server IP or FQDN></VPN_Server>`
	• Dans l'interface Web du téléphone, entrez l'adresse IP ou le FQDN du serveur VPN.
	Valeur par défaut : vide

VPN Utilisateur Name	Nom d'utilisateur pour un utilisateur d'accréditation sur le serveur VPN. 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 : `<VPN_User_Name ua="rw">Example</VPN_User_Name>` • Sur l'interface Web du téléphone, saisissez le nom d'utilisateur. Valeur par défaut : vide

Paramètre	Description et valeur par défaut
VPN Password	Mot de passe du nom d'utilisateur spécifié pour accéder au serveur VPN. 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 : `<VPN_Password ua="rw">Example</VPN_Password>` • Sur l'interface Web du téléphone, saisissez le mot de passe. Valeur par défaut : vide
Groupe de tunnels VPN	Groupe de tunnels attribué à l'utilisateur du VPN. Le groupe Tunnel est utilisé pour identifier la stratégie de groupe pour la connexion VPN. 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 : `<VPN_Tunnel_Group ua="rw">Example</VPN_Tunnel_Group>` • Dans l'interface Web du téléphone, saisissez le nom du groupe de tunnels. Valeur par défaut : vide
Se connecter au démarrage	Active ou désactive la connexion automatique au serveur VPN après le redémarrage du téléphone. 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 : `<Connect_on_Bootup ua="rw">No</Connect_on_Bootup>` • Sur l'interface Web du téléphone, définissez ce champ sur Oui ou Non en fonction des besoins. Valeurs autorisées : Oui et Non. Par défaut : Non

Présentation de la sécurité des produits Cisco

Ce produit, qui contient des fonctions cryptographiques, est soumis aux lois des États-Unis et d'autres pays, qui en régissent l'importation, l'exportation, le transfert et l'utilisation. La fourniture de produits cryptographiques Cisco n'autorise pas un tiers à importer, à exporter, à distribuer ou à utiliser le chiffrement. Les importateurs, exportateurs, distributeurs et utilisateurs sont responsables du respect des lois des États-Unis et des autres pays. En utilisant ce produit, vous acceptez de vous conformer aux lois et aux réglementations en vigueur. Si vous n'êtes pas en mesure de respecter les lois des États-Unis et celles des autres pays, renvoyez-nous ce produit immédiatement.

Pour en savoir plus sur les réglementations américaines sur les exportations, reportez-vous à l'adresse https://www.bis.doc.gov/policiesandregulations/ear/index.htm.