



# **Installation du téléphone H.323 IP Office Platform**

Version 11.1 FP2  
Édition 3  
Novembre 2021

# Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

© 2021, Avaya Inc.  
Tous droits réservés.

## Avis

Toutes les mesures nécessaires ont été prises pour garantir l'exactitude et la pertinence des informations contenues dans ce document au moment de son impression. Avaya Inc. ne peut cependant être tenu responsable des éventuelles erreurs ou omissions. Avaya se réserve le droit de modifier et de corriger les informations contenues dans ce document, sans devoir en informer qui que ce soit, ni quelque organisation que ce soit.

## Avis de limite de responsabilité en matière de documentation

Le terme « documentation » désigne l'ensemble des informations publiées sur divers supports, notamment les informations relatives aux produits, les instructions d'utilisation et les spécifications techniques de performance mis généralement à la disposition des utilisateurs des produits. Le terme documentation n'inclut pas les documents marketing. Avaya n'est pas responsable des modifications, ajouts ou suppressions réalisés par rapport à la version originale publiée de la documentation, sauf si ces modifications, ajouts ou suppressions ont été effectués par Avaya ou expressément en son nom. L'utilisateur final accepte d'indemniser et de ne pas poursuivre Avaya, ses agents et ses employés pour toute plainte, action en justice, demande et jugement résultant de ou en rapport avec des modifications, ajouts ou suppressions dans la mesure où celles-ci sont effectuées par l'utilisateur final.

## Avis de limite de responsabilité en matière de liens hypertextes

Avaya décline toute responsabilité quant au contenu et à la fiabilité des sites Web indiqués sur ce site ou dans les documents fournis par Avaya. Avaya décline toute responsabilité quant à l'exactitude des informations, des affirmations ou du contenu fournis par ces sites et n'approuve pas nécessairement les produits, services ou informations qui y sont décrits ou proposés. Avaya ne garantit pas que ces liens fonctionnent en toute circonstance et n'a aucun contrôle sur la disponibilité des pages Web en question.

## Garantie

Avaya offre une garantie limitée sur le matériel et les logiciels Avaya. Consultez votre contrat de vente pour en connaître les termes. Vous trouverez également les conditions générales de garantie pratiquées par Avaya, ainsi que des informations relatives à la prise en charge du produit, pendant la période de garantie, sur le site Web de support technique d'Avaya à l'adresse suivante : <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> sous la rubrique « Warranty & Product Lifecycle », ou sur le site successeur désigné par Avaya. Veuillez noter que si vous vous êtes procuré ce ou ces produits auprès d'un partenaire de distribution Avaya agréé en dehors des États-Unis et du Canada, la garantie vous est proposée par le partenaire de distribution Avaya agréé et non par Avaya.

Le terme « **service hébergé** » désigne un abonnement à un service hébergé Avaya souscrit auprès d'Avaya ou d'un partenaire de distribution Avaya agréé (le cas échéant), décrit ci-après dans la section relative au SAS hébergé et dans tout autre document décrivant le service hébergé applicable. Si vous souscrivez un abonnement à un Service hébergé, la garantie limitée susmentionnée peut ne pas s'appliquer, mais vous pouvez avoir droit aux services d'assistance liés au Service hébergé, tels que décrits ci-après dans vos documents décrivant le service hébergé applicable. Pour obtenir des informations complémentaires, contactez Avaya ou le partenaire de distribution Avaya (le cas échéant).

## Service hébergé

LES CONDITIONS SUIVANTES S'APPLIQUENT UNIQUEMENT LORSQUE VOUS ACHETEZ UN ABONNEMENT DE SERVICE HÉBERGÉ AVAYA AUPRÈS D'AVAYA OU D'UN PARTENAIRE AVAYA (LE CAS ÉCHÉANT). LES CONDITIONS D'UTILISATION DES SERVICES HÉBERGÉS SONT DISPONIBLES SUR LE SITE AVAYA, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) SOUS LE LIEN « Avaya Terms Of Use For Hosted Services » OU UN AUTRE SITE SUCCESSEUR TEL QUE DÉSIGNÉ PAR AVAYA, ET SONT APPLICABLES À TOUTE PERSONNE QUI ACCÈDE AU SERVICE HÉBERGÉ OU L'UTILISE. EN ACCÉDANT AU SERVICE HÉBERGÉ OU EN L'UTILISANT, OU EN AUTORISANT D'AUTRES À LE FAIRE, VOUS, EN VOTRE NOM, ET L'ENTREPRISE AU NOM DE LAQUELLE VOUS LE FAITES (CI-APRÈS DÉNOMMÉ INDIFFÉREMMENT COMME « VOUS » ET « UTILISATEUR FINAL »), ACCEPTEZ LES CONDITIONS

D'UTILISATION. SI VOUS ACCEPTEZ LES CONDITIONS D'UTILISATION AU NOM D'UNE ENTREPRISE OU AUTRE ENTITÉ JURIDIQUE, VOUS DÉCLAREZ QUE VOUS ÊTES HABILITÉ À LIER CETTE ENTITÉ À CES CONDITIONS D'UTILISATION. SI VOUS N'ÊTES PAS HABILITÉ À LE FAIRE OU SI VOUS NE SOUHAITEZ PAS ACCEPTER CES CONDITIONS D'UTILISATION, VOUS NE DEVEZ NI ACCÉDER AU SERVICE HÉBERGÉ, NI L'UTILISER, NI AUTORISER QUICONQUE À Y ACCÉDER OU À L'UTILISER.

## Licences

LES CONDITIONS DE LA LICENCE DU LOGICIEL DISPONIBLES SUR LE SITE INTERNET D'AVAYA ([HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo)) EN SUIVANT LE LIEN « CONDITIONS DE LA LICENCE DU LOGICIEL AVAYA (produits Avaya) » OU SUR LE SITE SUCCESSEUR DÉSIGNÉ PAR AVAYA, S'APPLIQUENT À QUICONQUE TÉLÉCHARGE, UTILISE ET/OU INSTALLE LE LOGICIEL AVAYA, ACQUIS AUPRÈS D'AVAYA INC., À TOUTE FILIALE D'AVAYA OU À TOUT PARTENAIRE DE DISTRIBUTION AVAYA (LE CAS ÉCHÉANT) SOUS CONTRAT COMMERCIAL AVEC AVAYA OU UN PARTENAIRE DE DISTRIBUTION AVAYA. SAUF STIPULATION CONTRAIRE ET SOUS RÉSERVE DE L'ACCORD ÉCRIT D'AVAYA, AVAYA NE PROPOSE PAS CETTE LICENCE SI LE LOGICIEL A ÉTÉ OBTENU AILLEURS QUE CHEZ AVAYA, UN AFFILIÉ AVAYA OU UN PARTENAIRE DE DISTRIBUTION AVAYA ; AVAYA SE RÉSERVE LE DROIT DE POURSUIVRE EN JUSTICE TOUTE PERSONNE UTILISANT OU VENDANT CE LOGICIEL SANS LICENCE. EN INSTALLANT, TÉLÉCHARGEANT OU UTILISANT LE LOGICIEL, OU EN AUTORISANT D'AUTRES PERSONNES À LE FAIRE, VOUS ACCEPTEZ, EN VOTRE PROPRE NOM ET AU NOM DE L'ENTITÉ POUR LAQUELLE VOUS INSTALLEZ, TÉLÉCHARGEZ OU UTILISEZ LE LOGICIEL (CI-APRÈS APPELÉE DE MANIÈRE INTERCHANGEABLE « VOUS » ET « UTILISATEUR FINAL »), CES CONDITIONS GÉNÉRALES ET D'ÊTRE LIÉ PAR CONTRAT AVEC AVAYA INC. OU L'AFFILIÉ D'AVAYA APPLICABLE (AVAYA). OU TOUTE AUTRE SOCIÉTÉ AFFILIÉE D'AVAYA CONCERNÉE (« AVAYA »).

Avaya vous accorde une licence d'exploitation couvrant les types de licence décrits ci-dessous, à l'exception des logiciels Heritage Nortel, pour lequel le champ d'application de la licence est détaillé ci-dessous. Lorsque le type de licence n'est pas expressément indiqué dans le document de commande, la licence applicable se rapporte à la licence système désigné, conformément aux termes de la section licence systèmes désignés (SD) ci-dessous, selon le cas. Le nombre de licences et d'unités de capacité pour lesquelles la licence est accordée est de un (1), sauf si un nombre différent de licences ou d'unités de capacité est spécifié dans la documentation ou d'autres textes mis à votre disposition. Le terme « logiciel » se rapporte aux programmes informatiques en code exécutable fournis par Avaya ou par un de ses partenaires de distribution, qu'il s'agisse de produits indépendants ou déjà installés sur du matériel ou de toute mise à niveau, mise à jour, correction de bogue ou version modifiée. « Processeur désigné » désigne un unique ordinateur autonome. « serveur » désigne un ensemble de processeurs désignés hébergeant (de façon physique ou virtuelle) une application logicielle accessible par plusieurs utilisateurs. Le terme « Instance » désigne un exemplaire unique du logiciel en cours d'exécution à un moment particulier : (i) sur une machine physique ; ou sur une machine virtuelle logicielle (« VM ») ou déploiement similaire.

## Type(s) de licence

Licence de système(s) désigné(s) (DS). L'utilisateur final est habilité à installer et utiliser chaque copie ou instance du logiciel uniquement : 1) sur un certain nombre de processeurs désignés, dans la limite indiquée dans la commande ; ou 2) dans la limite du nombre d'instances du logiciel indiquée dans la commande ou la documentation, ou conformément à l'autorisation écrite d'Avaya. Avaya se réserve le droit d'exiger que le ou les processeurs désignés soient identifiés sur la commande par type, numéro de série, code de caractéristique, Instance, emplacement ou toute autre désignation spécifique, ou fournis par l'utilisateur final à Avaya par un moyen électronique mis en place par Avaya spécifiquement à cette fin.

Licence utilisateur simultané (CU). L'utilisateur final peut installer et utiliser le logiciel sur plusieurs processeurs désignés ou serveurs tant que seul le nombre autorisé d'unités accède au logiciel et l'utilise à tout moment spécifié, conformément aux termes de la commande, de la documentation ou de l'autorisation écrite d'Avaya. Une « unité » représente l'unité sur laquelle Avaya, à son entière discrétion, base la tarification de ses licences et peut être, entre autres, un agent, un port, un utilisateur, un compte de

messagerie électronique ou un compte de messagerie vocale associé à un nom de personne ou à une fonction de l'entreprise (ex. : webmestre ou centre d'assistance) ou encore une entrée du répertoire dans la base de données administrative utilisée par le logiciel et autorisant un utilisateur à accéder à l'interface du logiciel. Les unités peuvent être associées à un serveur identifié spécifique ou à une instance du logiciel.

Licence en cluster (LC). L'utilisateur final est habilité à installer et à utiliser chaque copie ou instance du logiciel uniquement dans la limite du nombre de clusters indiquée dans la commande. Si cela n'est pas spécifié, il est possible d'installer un (1) cluster par défaut.

Licence entreprise (EN). L'utilisateur final est habilité à installer et à utiliser chaque copie ou instance du logiciel uniquement dans le cadre d'une utilisation à l'échelle de l'entreprise d'un nombre illimité d'instances du logiciel, conformément aux termes de la commande, de la documentation ou de l'autorisation écrite d'Avaya.

Licence utilisateur nommé (UN). L'utilisateur final peut : (i) installer et utiliser chaque copie ou sur un seul processeur désigné ou un seul serveur par utilisateur nommé autorisé (tel que défini ci-après) ; ou (ii) installer et utiliser chaque copie ou instance du logiciel sur un serveur dans la mesure où seuls les utilisateurs nommés autorisés accèdent au logiciel et l'utilisent conformément aux termes de la commande, de la documentation ou de l'autorisation écrite d'Avaya. Un « utilisateur nommé » est un utilisateur ou un dispositif qui a été expressément autorisé par Avaya à accéder au logiciel et à l'utiliser. Un « utilisateur nommé » peut être, à l'entière discrétion d'Avaya et sans limitation, désigné par son nom, sa fonction dans l'entreprise (par exemple, webmestre ou centre d'assistance), un compte de messagerie électronique ou vocale au nom d'une personne ou d'une fonction dans l'entreprise, ou d'une entrée de répertoire dans la base de données administrative utilisée par le logiciel et autorisant un seul utilisateur à la fois à accéder au logiciel.

Licence Shrinkwrap. L'utilisateur final peut installer et utiliser le logiciel en vertu des conditions des accords de licence applicables, tels qu'une licence « shrinkwrap » (acceptée par rupture de l'emballage) ou « clickthrough » (acceptée par lecture du contrat avant téléchargement) accompagnant le logiciel ou applicable à celui-ci (« Licence Shrinkwrap ») conformément aux termes de la commande, de la documentation ou de l'autorisation écrite d'Avaya.

Licence de transaction (TR) L'utilisateur final peut utiliser le logiciel jusqu'à concurrence du nombre de transactions spécifié pour une période limitée conformément aux termes de la commande, de la documentation ou de l'autorisation écrite d'Avaya. Une « transaction » désigne l'unité par laquelle Avaya, à sa seule discrétion, base la tarification de ses licences. Elle peut, sans limitation, être mesurée en fonction de l'utilisation, de l'accès, des interactions (entre client/serveur ou client/entreprise) ou du fonctionnement du logiciel dans une période de temps spécifiée (par exemple, par heure, par jour, par mois). Certains exemples de transactions incluent, sans y être limités, chaque message d'accueil/d'attente diffusé, chaque promotion personnalisée (sur n'importe quel canal), chaque opération de rappel, chaque agent en direct ou session de discussion en ligne, chaque appel acheminé ou redirigé (sur n'importe quel canal). L'utilisateur final ne peut dépasser le nombre de transactions sans le consentement préalable d'Avaya et le paiement de frais supplémentaires.

#### **Logiciels Heritage Nortel**

La mention « logiciels Heritage Nortel » signifie que le logiciel a été acheté par Avaya dans le cadre du rachat de Nortel Enterprise Solutions Business au mois de décembre 2009. Les logiciels Nortel hérités sont ceux présents dans la liste des produits Nortel hérités que vous trouverez à l'adresse <https://support.avaya.com/LicenselInfo> à l'aide du lien « produits Nortel hérités » ou sur un site successeur désigné par Avaya. Pour les logiciels Heritage Nortel, Avaya accorde au client une licence d'utilisation des logiciels Heritage Nortel fournis ci-dessous, uniquement pour le niveau d'activation ou d'utilisation autorisé, uniquement aux fins spécifiées dans la documentation, et uniquement intégrés à, pour exécution sur ou pour communication avec les équipements Avaya. Les frais concernant les logiciels Heritage Nortel peuvent porter sur une extension d'activation ou d'utilisation autorisée telle que spécifiée dans un bon de commande ou un devis.

#### **Copyright**

Sauf mention contraire explicite, il est interdit d'utiliser les documents disponibles sur ce site ou dans la documentation, les

logiciels, le service hébergé ou le matériel fournis par Avaya. Tout le contenu de ce site, toute documentation, Service hébergé et tout produit fournis par Avaya, y compris la sélection, la disposition et la conception du contenu, appartient à Avaya ou à ses concédants de licence et est protégé par les droits d'auteur et autres droits sur la propriété intellectuelle, y compris les droits sui generis de protection des bases de données. Vous ne pouvez pas modifier, copier, reproduire, republier, télécharger, déposer, transmettre ou distribuer, de quelque façon que ce soit, tout contenu, partiel ou intégral, y compris tout code et logiciel sans l'autorisation expresse d'Avaya. La reproduction, la transmission, la diffusion, le stockage et/ou l'utilisation non autorisés de cette documentation sans l'autorisation expresse d'Avaya peuvent constituer un délit passible de sanctions civiles ou pénales en vertu des lois en vigueur.

#### **Virtualisation**

Ce qui suit s'applique si le produit est déployé sur une machine virtuelle. Chaque produit possède un code de commande et des types de licence spécifiques. Sauf mention contraire, chaque instance de produit doit faire l'objet d'une licence distincte et être commandée séparément. Par exemple, si l'utilisateur final ou le partenaire de distribution Avaya souhaite installer deux instances du même type de produits, il est nécessaire de commander deux produits de ce type.

#### **Composants tiers**

Le terme « composants tiers » signifie que certains logiciels ou certaines parties des logiciels inclus dans le logiciel ou le service hébergé peuvent contenir des composants logiciels (y compris des composants open source) distribués dans le cadre de contrats avec des tiers (« composants tiers ») faisant l'objet de conditions quant aux droits d'utilisation de certaines parties du logiciel (« conditions tierces »). Les informations portant sur le code source du SE Linux (pour les Produits ayant distribué le code source du SE Linux) et identifiant les titulaires de copyright des composants tiers et les Termes tiers en vigueur sont disponibles dans les produits, dans la documentation ou sur le site Web d'Avaya à l'adresse : <https://support.avaya.com/Copyright> ou tout site successeur désigné par Avaya. Les conditions de licence des logiciels libres fournies dans le cadre des conditions tierces sont cohérentes avec les droits de licence concédés dans ces conditions de licence de logiciel, et peuvent vous accorder des droits supplémentaires tels que la modification et la distribution des logiciels libres. Les conditions tierces prévaudront sur les conditions de licence de logiciel, uniquement en ce qui concerne les composants tiers applicables, si ces conditions de licence de logiciel imposent des restrictions plus importantes que celles des conditions tierces applicables.

Les dispositions suivantes s'appliquent uniquement lorsque le codec H.264 (AVC) est fourni avec le produit. CE PRODUIT FAIT L'OBJET D'UNE LICENCE DE PORTEFEUILLE DE BREVETS AVC POUR L'UTILISATION PERSONNELLE ET NON COMMERCIALE PAR UN PARTICULIER POUR (i) ENCODER DE LA VIDÉO SELON LA NORME AVC (« VIDÉO AVC ») ET/OU (ii) DÉCODER DE LA VIDÉO AVC ENCODÉE PAR UN PARTICULIER ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET/OU OBTENUE AUPRÈS D'UN FOURNISSEUR DE VIDÉOS HABILITÉ À FOURNIR DES VIDÉOS AVC. AUCUNE LICENCE N'EST OCTROYÉE DE FAÇON EXPLICITE OU IMPLICITE POUR TOUTE AUTRE UTILISATION. DES INFORMATIONS SUPPLÉMENTAIRES SONT DISPONIBLES AUPRÈS DE MPEG LA, L.L.C. ([HTTP://WWW.MPEGLA.COM](http://www.mpegla.com)).

#### **Fournisseur de service**

CELA S'APPLIQUE À L'HÉBERGEMENT DES PRODUITS OU SERVICES AVAYA PAR LES PARTENAIRES DE DISTRIBUTION D'AVAYA. LE PRODUIT OU SERVICE HÉBERGÉ PEUT UTILISER DES ÉLÉMENTS TIERS QUI SONT SUJETS À DES CONDITIONS DE TIERS ET QUI NÉCESSITENT UN FOURNISSEUR DE SERVICES POUR OBTENIR LA LICENCE INDÉPENDamment ET DIRECTEMENT AUPRÈS D'UN FOURNISSEUR TIERS. L'HÉBERGEMENT DES PRODUITS AVAYA PAR LES PARTENAIRES DE DISTRIBUTION D'AVAYA DOIT ÊTRE AUTORISÉ PAR ÉCRIT PAR AVAYA ET SI CES PRODUITS UTILISENT OU INCORPorent CERTAINS LOGICIELS TIERS, Y COMPRIS, SANS S'Y LIMITER, LES LOGICIELS OU CODECS MICROSOFT, LE PARTENAIRE DE DISTRIBUTION D'AVAYA DOIT OBTENIR INDÉPENDamment TOUT ACCORD DE LICENCE APPLICABLE, À SES FRAIS, DIRECTEMENT AUPRÈS DU FOURNISSEUR TIERS APPLICABLE.

CONCERNANT LES CODECS, SI LE PARTENAIRE DE DISTRIBUTION D'AVAYA HÉBERGE UN PRODUIT QUI UTILISE

OU INCORPORE LE CODEC H.264 OU H.265, LE PARTENAIRE DE DISTRIBUTION D'AVAYA RECONNAÎT ET ACCEPTE QUE LE PARTENAIRE DE DISTRIBUTION D'AVAYA EST RESPONSABLE POUR TOUS LES FRAIS ET/OU DROITS D'AUTEUR RELATIFS. LE CODEC H.264 (AVC) FAIT L'OBJET D'UNE LICENCE DE PORTEFEUILLE DE BREVETS AVC POUR L'UTILISATION PERSONNELLE ET NON COMMERCIALE PAR UN PARTICULIER POUR (I) ENCODER DE LA VIDÉO SELON LA NORME AVC (« VIDÉO AVC ») ET/OU (II) DÉCODER DE LA VIDÉO AVC ENCODÉE PAR UN PARTICULIER ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET/OU OBTENUE AUPRÈS D'UN FOURNISSEUR DE VIDÉOS HABILITÉ À FOURNIR DES VIDÉOS AVC. AUCUNE LICENCE N'EST OCTROYÉE DE FAÇON EXPLICITE OU IMPLICITE POUR TOUTE AUTRE UTILISATION. VOUS POUVEZ OBTENIR DES INFORMATIONS SUPPLÉMENTAIRES POUR LES CODECS H.264 (AVC) ET H.265 (HEVC) DEPUIS MPEG LA, L.L.C. ([HTTP://WWW.MPEGLA.COM](http://www.mpegla.com)).

### **Dans le respect des lois**

Vous reconnaissez et acceptez être tenu responsable de vous conformer aux lois et règlements applicables, y compris, sans s'y limiter, les lois et règlements en lien avec l'enregistrement des appels, la confidentialité des données, la propriété intellectuelle, le secret commercial, la fraude et les droits d'interprétation musicale du pays ou du territoire dans lequel le produit Avaya est utilisé.

### **Lutte contre la fraude à la tarification**

Le terme « fraude à la tarification » fait référence à l'usage non autorisé de votre système de télécommunication par un tiers non habilité (par exemple, une personne qui ne fait pas partie du personnel de l'entreprise, qui n'est ni agent, ni sous-traitant ou qui ne travaille pas pour le compte de votre société). Sachez que votre système peut faire l'objet d'une fraude à la tarification et qu'en cas de fraude, les frais supplémentaires pour vos services de télécommunications peuvent être importants.

### **Intervention en cas de fraude à la tarification**

Si vous pensez être victime d'une fraude à la tarification et nécessitez une assistance technique ou autre, contactez l'assistance d'intervention en cas de fraude à la tarification au 1-800-643-2353 (États-Unis et Canada). Pour obtenir d'autres numéros de téléphone d'assistance, reportez-vous au site Web de support technique d'Avaya : <https://support.avaya.com>, ou au site successeur désigné par Avaya.

### **Faibles de sécurité**

Vous trouverez plus d'informations concernant la politique d'assistance d'Avaya en matière de sécurité dans la rubrique Politique de sécurité et assistance (<https://support.avaya.com/security>).

Les failles sécuritaires suspectées du produit sont traitées conformément au processus d'assistance sécuritaire pour les produits Avaya (<https://support.avaya.com/css/P8/documents/100161515>).

### **Marques de commerce**

Les marques de commerce, les logos et les marques de service (« marques ») figurant sur ce site, sur toute documentation, le ou les services hébergés et sur tout produit fournis par Avaya sont des marques déposées ou non déposées d'Avaya, de ses sociétés affiliées, de ses concédants de licences, de ses fournisseurs ou de parties tierces. Les utilisateurs ne sont pas autorisés à utiliser ces marques sans autorisation écrite préalable d'Avaya ou dudit tiers qui peut être propriétaire de la Marque. Rien de ce qui est contenu dans ce site, la documentation, le ou les services hébergés et le ou les produits ne saurait être interprété comme accordant, par implication, préclusion ou autrement, toute licence ou tout droit sur les marques sans l'autorisation écrite expresse d'Avaya ou du tiers applicable.

Avaya est une marque commerciale déposée d'Avaya Inc.

Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Linux<sup>®</sup> est une marque de commerce déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

## Sommaire

<b>Partie 1 : Installation du téléphone H323 IP Office</b> .....	9
<b>Chapitre 1 : Téléphones IP H.323 IP Office</b> .....	10
Nouveautés de cette version.....	11
Téléphones IP H.323 pris en charge.....	11
Capacité du système.....	12
Firmware du téléphone.....	13
Génération automatique du fichier.....	14
Installation simple.....	14
Conditions requises pour l'installation.....	16
Licences et abonnements.....	18
Évaluation du réseau.....	18
Canaux de compression de voix.....	19
QoS.....	21
Problèmes VoIP potentiels.....	22
Connexion au PC utilisateur.....	23
Options d'alimentation.....	23
Options du serveur de fichiers.....	24
Cartes mémoire de l'unité de contrôle.....	26
Demandes de fichiers du téléphone.....	26
Génération automatique du fichier.....	27
Carte mémoire de l'unité de contrôle.....	28
Mise sur liste noire des enregistrements.....	28
Blocage des codes d'accès par défaut.....	28
<b>Chapitre 2 : Paramètres supplémentaires du téléphone</b> .....	30
46xxspecials.txt.....	31
NoUser Source Numbers.....	32
Configuration et modification des paramètres des fichiers.....	33
<b>Partie 2 : Processus d'installation de base</b> .....	35
Installation du téléphone IP H.323.....	35
<b>Chapitre 3 : Licences et abonnements</b> .....	37
Réservation des licences.....	37
<b>Chapitre 4 : Activation du responsable de passerelle H.323</b> .....	39
Configuration de la plage de ports RTP.....	39
Paramétrage de la qualité de service (QoS) de DiffServ.....	41
Codecs par défaut du système.....	41
<b>Chapitre 5 : Paramètres DHCP</b> .....	43
Prise en charge DHCP du système.....	43
Numéros d'option spécifiques aux sites du système.....	44
Modification des paramètres SSON du système.....	44
<b>Chapitre 6 : Paramètres du serveur de fichiers</b> .....	46
Modification des paramètres du serveur de fichiers.....	47
Paramètres du serveur de fichiers des téléphones.....	48

Créer/Modifier le fichier de paramètres.....	48
Modification manuelle du fichier.....	50
Chargement de fichiers logiciels dans le système.....	50
Unité de contrôle IP500 V2.....	51
Utilisation du gestionnaire de fichiers intégré pour vérifier/charger les fichiers.....	51
Copie manuelle des fichiers.....	52
Chargement de fichiers sur un serveur tiers.....	53
<b>Chapitre 7 : Création des utilisateurs et des postes.....</b>	<b>54</b>
Mot de passe par défaut du poste.....	54
Création manuelle des utilisateurs.....	55
Création manuelle de postes.....	56
Sélection du codec requis.....	56
Utilisation de l'auto-création automatique.....	57
<b>Chapitre 8 : Connexion du téléphone.....</b>	<b>59</b>
Enregistrement du téléphone.....	60
Liste des téléphones enregistrés.....	61
<b>Partie 3 : Configuration facultative.....</b>	<b>62</b>
<b>Chapitre 9 : Activation de la surveillance de la qualité du protocole RTCP.....</b>	<b>63</b>
Activation des rapports de qualité sur les téléphones.....	63
Activation des rapports de qualité du système.....	64
Configuration des seuils d'alarme de qualité.....	65
<b>Chapitre 10 : Économiseur d'écran.....</b>	<b>66</b>
Personnalisation des paramètres de l'économiseur d'écran.....	67
<b>Chapitre 11 : Paramètres de sauvegarde/restauration.....</b>	<b>68</b>
Définition de la valeur BRURI.....	69
Authentification HTTP.....	69
Gestion manuelle des opérations de sauvegarde/restauration.....	70
Exemple de fichier.....	70
Configuration du serveur IIS.....	72
Configuration du serveur Apache.....	72
<b>Partie 4 : Processus d'installation avancés.....</b>	<b>74</b>
<b>Chapitre 12 : Installation d'adresses statiques.....</b>	<b>75</b>
Installation de l'adresse statique pour les téléphones de la série 1600.....	75
Paramètres d'installation de l'adresse statique pour les téléphones de la série 1600.....	76
Installation de l'adresse statique pour les téléphones de la série 9600.....	77
Paramètres d'installation de l'adresse statique pour les téléphones de la série 9600.....	77
<b>Chapitre 13 : Postes H.323 distants.....</b>	<b>79</b>
Configuration du réseau client.....	80
Configuration du système IP Office *.....	81
Configuration des téléphones.....	82
<b>Chapitre 14 : Téléphones VPN distants.....</b>	<b>83</b>
Documentation d'installation.....	84
Micrologiciel du téléphone VPN distant pris en charge.....	84
Configuration du VPN distant sur un téléphone IP.....	85
VLAN et téléphones IP.....	85

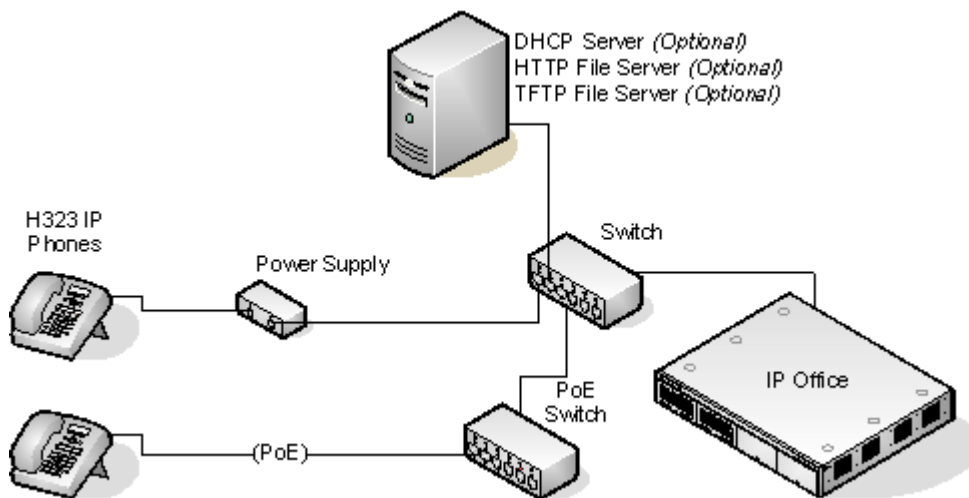
VLAN et DHCP.....	86
Exemple de configuration : présentation.....	87
Présentation d'un exemple de système.....	90
<b>Chapitre 15 : Autre configuration du serveur DHCP.....</b>	<b>92</b>
Autres options.....	92
Vérification de la prise en charge du serveur DHCP.....	94
Création d'un champ d'application.....	95
Ajout d'une option 242.....	96
Activation du champ d'application.....	97
<b>Chapitre 16 : Prise en charge du protocole SRTP.....</b>	<b>98</b>
Activation du protocole SRTP au niveau du système.....	98
Activation du protocole SRTP au niveau du système.....	99
Désactivation du protocole SRTP sur un poste ou une ligne.....	99
Support direct.....	100
<b>Chapitre 17 : Prise en charge du protocole TLS.....</b>	<b>101</b>
Modification du mot de passe CRAFT.....	102
Ajout du certificat d'identité.....	102
Téléchargement du certificat d'identité à partir d'un serveur Linux.....	103
Chargement d'un certificat dans le magasin de certificats approuvés du serveur.....	103
Activation de TLS sur le système IP Office.....	104
Activation de TLS sur les téléphones.....	104
Vérification du fonctionnement de TLS.....	105
<b>Partie 5 : Divers.....</b>	<b>106</b>
<b>Chapitre 18 : Options d'administration statique.....</b>	<b>107</b>
Utilisation des options d'administration statique.....	107
Saisie des options administratives sur les téléphones de la série 1600.....	108
Saisie des options administratives sur les téléphones de la série 9600.....	108
Mot de passe de processus administrateur.....	109
Activation de l'interface du concentrateur.....	109
Activation de l'interface du concentrateur pour les téléphones de la série 1600.....	110
Activation de l'interface du concentrateur pour la série 9600.....	110
Affichage des détails du téléphone.....	111
Affichage des détails des téléphones de la série 1600.....	111
Affichage des détails des téléphones de la série 9600.....	112
Procédure de test automatique pour les téléphones de la série 1600.....	113
Procédure de test automatique pour les téléphones de la série 9600.....	114
Réinitialisation d'un téléphone.....	114
Réinitialisation d'un téléphone de la série 1600.....	114
Réinitialisation du téléphone de la série 9600.....	115
Désactivation d'un téléphone.....	115
Désactivation des téléphones de la série 1600.....	116
Désactivation des téléphones de la série 9600.....	116
Numéro d'option spécifique au site.....	116
SSON sur les téléphones de la série 1600.....	117
SSON sur les téléphones de la série 9600.....	117
<b>Chapitre 19 : Scénarios de redémarrage.....</b>	<b>118</b>

Mise à jour nécessaire du fichier d'amorçage.....	119
Aucun fichier d'application ou mise à jour nécessaire du fichier d'application.....	119
Fichier d'amorçage correct et fichier d'application déjà chargé.....	120
<b>Chapitre 20 : Ressources</b> .....	121
Documentation.....	121
Recherche de documents sur le site Web du support technique d'Avaya.....	121
Formation.....	121
Visualiser les vidéos Avaya Mentor.....	121
Support technique.....	122
Utilisation de l'InSite Knowledge Base (base de connaissances sur site) d'Avaya....	122

# Partie 1 : Installation du téléphone H323 IP Office

# Chapitre 1 : Téléphones IP H.323 IP Office

Cette documentation fournit des instructions d'installation pour les téléphones IP Avaya pris en charge sur un système IP Office. Vous devez utiliser ce document conjointement à la documentation d'installation existante de ces téléphones.



- **Installation DHCP par rapport à IP statique** : même si l'installation IP statique des téléphones IP H.323 est possible, nous vous conseillons fortement une installation avec le protocole DHCP. L'utilisation de DHCP facilite le processus d'installation ainsi que l'entretien et l'administration à venir. Dans les installations statiques, après une mise à jour du fichier d'amorçage, tous les paramètres d'adresses statiques sont perdus et doivent être saisis à nouveau.
- **Évaluation du réseau** : une haute qualité de transmission vocale sur un réseau IP demande une évaluation de nombreux facteurs. Par conséquent :
  - Nous vous conseillons fortement de faire installer vos téléphones IP uniquement par des installateurs expérimentés en VoIP.
  - L'intégralité du réseau du client doit être évaluée avant l'installation pour établir s'il est compatible avec le système VoIP. Avaya ne prendra pas en charge d'installation s'il est impossible de fournir les résultats d'une évaluation de réseau. Pour plus d'informations, voir [Évaluation du réseau](#) à la page 18.

## Liens connexes

[Nouveautés de cette version](#) à la page 11

[Téléphones IP H.323 pris en charge](#) à la page 11

[Capacité du système](#) à la page 12

[Firmware du téléphone](#) à la page 13

- [Génération automatique du fichier](#) à la page 14
- [Installation simple](#) à la page 14
- [Conditions requises pour l'installation](#) à la page 16
- [Licences et abonnements](#) à la page 18
- [Évaluation du réseau](#) à la page 18
- [Canaux de compression de voix](#) à la page 19
- [QoS](#) à la page 21
- [Problèmes VoIP potentiels](#) à la page 22
- [Connexion au PC utilisateur](#) à la page 23
- [Options d'alimentation](#) à la page 23
- [Options du serveur de fichiers](#) à la page 24
- [Cartes mémoire de l'unité de contrôle](#) à la page 26
- [Demandes de fichiers du téléphone](#) à la page 26
- [Carte mémoire de l'unité de contrôle](#) à la page 28
- [Mise sur liste noire des enregistrements](#) à la page 28
- [Blocage des codes d'accès par défaut](#) à la page 28

---

## Nouveautés de cette version

Ce manuel présente les modifications suivantes intégrées à IP Office version 11.1 :

- Fonctionnement du mode abonnement : les systèmes IP Office peuvent désormais fonctionner en mode abonnement. Dans ce mode, les droits de licence des téléphones IP pour le système sont accordés par un utilisateur abonné plutôt que par une licence de poste. Le mode abonnement ne prend en charge que les téléphones Avaya H323 suivants :
  - Série 1600 : 1603IP/SW, 1608, 1608-I, 1616, 1616-I
  - Série 3600 : 3641, 3645
  - Série 3700 : 3720, 3725, 3730, 3735, 3740, 3745, 3749 : connexion via les stations de base DECT R4.
  - Série 9600 : 9608, 9608G, 9611G, 9621G, 9641G, 9641GS.

### Liens connexes

- [Téléphones IP H.323 IP Office](#) à la page 10

---

## Téléphones IP H.323 pris en charge

Cette documentation fournit des notes d'installation pour les téléphones Avaya suivants. Les autres téléphones IP H.323 d'Avaya pris en charge, par exemple les téléphones de la série DECT R4 3700, sont abordés dans un document d'installation distinct.

Téléphones IP H.323		Classe PoE		Port du PC	Mode d'abonnement
		PoE	Inactif		
Série 1600	1603	2	4,4 W	-	✓
	1603SW	2	4,4 W	✓	✓
	1608	2	3,7 W	✓	✓
	1616	2	2,7 W	✓	✓
Série 9600	9608	1	2,08 W	✓	✓
	9611G	1	2,8 W	✓	✓
	9621G	2	3,49 W	✓	✓
	9641G	2	3,44 W	✓	✓

- 1603/1603SW : ces téléphones nécessitent un séparateur d'alimentation PoE pour être alimentés de cette manière.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Capacité du système

La capacité du système englobe le nombre de postes téléphoniques configurables et le nombre d'appels téléphoniques IP simultanés.

### Capacité des extensions

Le nombre maximum de téléphones H.323 IP pris en charge dépend du type de système.

Les systèmes IP500 V2 prennent en charge jusqu'à 384 postes. Pour connaître la capacité en téléphones IP, retranchez le nombre de ports de postes installés sur le système qui ne sont pas des postes IP, c'est à dire, les ports de postes de l'unité de contrôle IP Office et tous les modules d'expansion externes. Veuillez noter toutefois que ces systèmes prennent uniquement en charge un maximum de 148 canaux VCM, ce qui peut également limiter le nombre d'appels VoIP simultanés ; voir ci-dessous.

Pour les systèmes IP Office Server Edition, la capacité en matière de postes IP dépend du type de serveur. Reportez-vous au document [Directives de la plateforme Avaya IP Office™ : capacité](#).

### Capacité d'appels

Il existe un certain nombre de situations dans lesquelles le système IP500 V2 doit fournir un canal de compression vocale pour qu'un téléphone IP puisse passer des appels. Les canaux de compression vocale sont fournis par les modules de compression vocale (VCM) installés sur le système. Le nombre de canaux VCM requis et la longueur de canal nécessaire dépendent d'un certain nombre de facteurs.

En résumé, on peut dire que :

- Un canal VCM est requis lors de la configuration des appels.
- Le canal VCM est libéré si l'appel provient de/est destiné à un autre périphérique IP qui utilise le même codec de compression (les codecs VCM pris en charge sont G.711, G.729 et G.722).

- Le canal VCM est utilisé pour toute la durée de l'appel quand l'appel est destiné à/ provient de/passe par un périphérique qui n'est pas IP (poste ou ligne réseau).
- Il ne faut pas oublier que les canaux VCM servent également aux appels qui proviennent de périphériques non-IP destinés à des lignes IP, si celles-ci sont configurées dans le système IP Office (lignes IP, SIP et SES).
- Les appels provenant de téléphones IP et à destination du serveur de la messagerie vocale IP Office utilisent un canal VCM.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

## Firmware du téléphone

Le micrologiciel des téléphones IP d'Avaya peut être mis à niveau et différentes versions du micrologiciel sont disponibles sur le site Web d'assistance d'Avaya. Cependant, les téléphones IP H.323 utilisés sur un système IP Office doivent uniquement utiliser le micrologiciel préinstallé dans le système IP Office ou fourni avec son application IP Office Manager. Il est possible que les autres versions du micrologiciel du téléphone IP n'aient pas été testées spécifiquement avec les systèmes IP Office. Dans ce cas, elles ne doivent pas être utilisées, excepté si l'assistance d'IP Office est spécifiquement mentionnée dans la documentation qui accompagne le micrologiciel.

Le micrologiciel se compose de plusieurs types de fichiers :

Type de fichier	Description
Fichiers xxupgrade	<p>Le premier fichier demandé par un téléphone lors de son démarrage est le fichier xxupgrade. Ce fichier contient une liste des fichiers .bin du téléphone disponibles dans l'ensemble de firmware et des numéros de version de ces fichiers. Si la version d'un fichier diffère de celle téléchargée par le téléphone, celui-ci demandera le nouveau fichier.</p> <p>Au cours de cette procédure, il est possible que le téléphone redémarre après avoir chargé chaque fichier, puis demande à nouveau le fichier xxupgrade.txt jusqu'à ce qu'il ait mis à jour tous ses firmwares, si nécessaire. Des fichiers distincts sont fournis pour les différentes séries de téléphones. Par exemple :</p> <ul style="list-style-type: none"> <li>• 16xxupgrade.txt : ce fichier répertorie les fichiers du micrologiciel à charger par les téléphones de la série 1600.</li> <li>• 96xxupgrade.txt : ce fichier répertorie les fichiers du micrologiciel à charger par les téléphones de la série 9600.</li> <li>• 96x1Hupgrade.txt : ce fichier répertorie les fichiers du micrologiciel à charger par les téléphones des séries 9608, 9611, 9621 et 9641.</li> </ul>
Fichiers .bin	<p>En suivant les instructions contenues dans le fichier xxupgrade.txt, le téléphone charge les fichiers .bin dont il a besoin si leurs versions sont différentes de celles que le téléphone a déjà chargées.</p>

*Le tableau continue ...*

Type de fichier	Description
Fichiers .tar	À la place du fichier .bin utilisé par d'autres téléphones, les téléphones de la série 9600 utilisent les fichiers d'archive .tar pour télécharger plusieurs fichiers en une seule étape, puis les décompresse pour charger leur contenu.
Fichiers 46xxsettings.txt	La dernière ligne du fichier xxupgrade.txt demande au téléphone de charger un fichier 46xxsettings.txt. Il s'agit d'un fichier modifiable pouvant être utilisé pour ajuster le fonctionnement des téléphones.
Fichiers .lng	Le micrologiciel peut comprendre des fichiers de langue qui peuvent être utilisés par les téléphones des séries 1600 et 9600. Les fichiers de langue qui seront chargés sont définis dans le fichier 46xxsettings.txt.

Les fichiers du micrologiciel du téléphone sont installés en même temps que l'application IP Office Manager et se trouvent dans le répertoire d'installation de l'application. Par défaut, le répertoire se trouve ici : c:\Program Files\Avaya\IP Office\Manager.

Ces mêmes fichiers de micrologiciel peuvent également être obtenus via le package logiciel utilisé pour installer IP Office Manager sans avoir à procéder à l'installation. Les fichiers se trouvent dans le sous-dossier \program files\Avaya\IPOffice\Manager du répertoire d'installation.

Notez que ces ensembles de fichiers comportent des fichiers .bin qui sont également utilisés pour d'autres périphériques, notamment le système IP Office lui-même.

#### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Génération automatique du fichier

Lorsque le système IP Office est utilisé comme serveur de fichiers pour les téléphones, il peut créer automatiquement les fichiers 46xxsettings.txt et .lng qui seront utilisés par les téléphones. Cela a lieu si le fichier demandé n'est pas physiquement présent à l'emplacement où le système stocke les fichiers du firmware. Le système utilise également les paramètres de configuration de l'utilisateur pour créer automatiquement le fichier des paramètres de l'utilisateur du téléphone.

Le système peut créer automatiquement les fichiers même lorsque la redirection HTTP est utilisée pour charger les fichiers .bin des téléphones 9608, 9611, 9621 et 9641 depuis un autre serveur de fichiers.

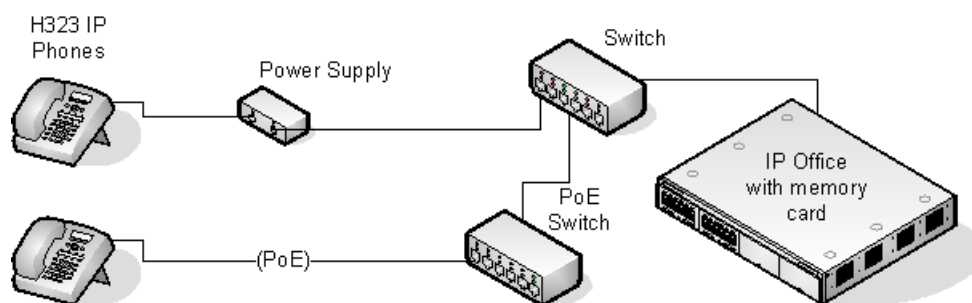
#### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Installation simple

Pour l'installation la plus simple, le système IP Office agit comme le serveur DHCP et les serveurs de fichiers pour l'ensemble des téléphones IP enregistrés.



Ce type d'installation utilise le matériel suivant :

- **Serveur IP Office** : le système IP Office a plusieurs rôles pour les téléphones :
  - **Serveur DHCP** : le système IP Office agit en tant que serveur DHCP pour les téléphones. La réponse DHCP reçue par les téléphones inclut les paramètres des adresses IP, les détails du serveur de fichiers à utiliser tel qu'il est configuré dans la configuration IP Office et les systèmes sur l'adresse de la passerelle H.323 des téléphones. La fonction DHCP d'IP Office peut être configurée pour fournir des adresses DHCP uniquement afin de répondre aux requêtes provenant des téléphones IP Avaya. Vous pouvez ainsi utiliser un autre serveur DHCP pour les autres périphériques qui utilisent DHCP.
  - **Responsable de passerelle H.323** : les téléphones IP doivent avoir un responsable de passerelle H.323 auprès duquel ils s'enregistrent. Le responsable de passerelle contrôle ensuite la connexion des appels vers et depuis le téléphone. Dans ce scénario et dans tous les cas, les systèmes IP Office fonctionnent comme celui du responsable de passerelle H.323.
  - **Serveur de fichiers** : lors de l'installation, les téléphones IP doivent télécharger des fichiers du micrologiciel depuis un serveur de fichiers. Pour ce faire, utilisez le protocole HTTPS, HTTP ou TFTP dans cet ordre (les téléphones des séries 1600 et 9600 ne prennent pas en charge le protocole TFTP). Vous pouvez utiliser la carte mémoire de l'unité de contrôle IP Office en tant que source de fichiers.
  - Les systèmes IP500 V2 peuvent servir de serveur de fichiers pour un maximum de 50 téléphones en utilisant leur propre carte mémoire. Les systèmes IP Office Server Edition peuvent également servir de serveur de fichiers pour un maximum de 50 téléphones. Pour des quantités plus importantes, un serveur HTTP tiers distinct doit être utilisé.
  - **Serveur de sauvegarde/restauration** : les téléphones des séries 1600 et 9600 peuvent être configurés pour sauvegarder et restaurer les paramètres des utilisateurs et des postes sur un serveur. L'adresse de ce serveur configurée séparément de celle du serveur de fichiers utilisé pour le micrologiciel du téléphone via le même serveur peut être utilisée. La méthode recommandée est le système IP Office en tant que serveur pour cette fonction.
- **Commutateurs** : IP Office possède un nombre limité de ports de connexion LAN uniquement destinés à se connecter au réseau de données existant. L'ajout de téléphones IP nécessite que le réseau dispose d'une capacité d'accueil de ports supplémentaires.

- **Alimentations** : chaque téléphone IP H.323 nécessite une alimentation. Le système IP Office n'alimente pas les téléphones IP. Les téléphones peuvent être alimentés de la façon suivante :
  - **Alimentation par câble Ethernet** : la plupart des téléphones IP Avaya peuvent utiliser une alimentation sur Ethernet (PoE) 802.3af. Pour ce faire, il est possible d'utiliser des commutateurs PoE pour prendre en charge plusieurs téléphones ou des périphériques à injecteur PoE individuels pour chaque téléphone.
  - **Adaptateurs d'alimentation individuels** : chaque téléphone peut utiliser un adaptateur d'alimentation individuel. Pour cela, vous aurez besoin d'une prise électrique à l'endroit où se trouve chaque téléphone. Le type d'alimentation varie en fonction du type de téléphone. Veuillez noter qu'il sera peut-être nécessaire d'utiliser une source d'alimentation individuelle pour les téléphones utilisant des modules de boutons, plutôt qu'une alimentation PoE.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Conditions requises pour l'installation

Pour installer un téléphone IP sur IP Office, les éléments suivants sont requis :

	Description
<b>Évaluation du réseau</b>	Une évaluation du réseau doit être effectuée. Avaya ne prend pas en charge la fonction VoIP sur les réseaux dont l'évaluation du réseau ne s'est pas avérée satisfaisante.
<b>Numéro de poste et détails de l'utilisateur</b>	Une liste complète du numéro de poste planifié et des détails concernant le nom de l'utilisateur est nécessaire. Le numéro de poste planifié ne doit pas être déjà utilisé et est demandé par le téléphone au cours de l'installation.
<b>Alimentations</b>	Chaque téléphone nécessite une alimentation. Les téléphones IP d'Avaya ne sont pas alimentés par IP Office. Plusieurs options sont proposées sur le mode d'alimentation des téléphones et la prise en charge de l'alimentation sur Ethernet (PoE) par l'ensemble des postes IP Avaya. Voir <a href="#">Options d'alimentation</a> à la page 23
<b>Prise LAN</b>	Un point de connexion LAN Ethernet RJ45 est requis pour chaque téléphone.
<b>Câblage de catégorie</b>	Tous les câbles LAN et les infrastructures de câbles LAN utilisés avec les téléphones IP H.323 doivent appartenir à la catégorie de câblage 5.
<b>Câbles LAN</b>	Vérifiez qu'un câble de réseau LAN RJ45 est fourni avec le téléphone IP, permettant de le raccorder à l'unité d'alimentation. Il vous faut également un deuxième câble LAN RJ45 pour connecter l'unité d'alimentation au réseau local du client. Cela dépend du type d'alimentation que vous utilisez.  Un câble LAN RJ45 supplémentaire peut être utilisé pour connecter le PC de l'utilisateur au réseau local par l'intermédiaire du téléphone IP (non pris en charge par les modèles de téléphones IP H.323 des séries 4601, 4602, 5601 et 5602).

*Le tableau continue ...*

	Description
<b>Canaux de compression de voix</b>	Sur les systèmes IP500 V2, l'unité de contrôle doit être installée avec des canaux de compression vocale. Les canaux sont obligatoires pour la phase de connexion si les appels impliquent des téléphones IP et peuvent également s'avérer nécessaires pendant l'appel. Pour plus d'informations, voir <a href="#">Canaux de compression de voix</a> à la page 19.
<b>Serveur DHCP</b>	L'unité IP Office peut remplir ce rôle pour tous les téléphones. Si un autre serveur DHCP est utilisé pour le réseau, il peut servir de protocole DHCP pour les téléphones IP H.323, voir Autres serveurs DHCP. De plus, le système IP Office peut être configuré pour fournir uniquement la prise en charge DHCP aux téléphones IP Avaya. <ul style="list-style-type: none"> <li>• Adressage IP statique : cette fonction peut également être utilisée pour l'installation des téléphones IP, si nécessaire. Toutefois, cette méthode d'installation n'est pas recommandée.</li> </ul>
<b>Serveur de fichiers HTTP</b>	Un PC qui exécute l'application IP Office Manager peut exercer ce rôle pour un maximum de 5 téléphones IP H.323. Une unité de contrôle IP Office dotée d'une carte mémoire peut utiliser cette carte mémoire comme source pour 50 téléphones maximum. Le système IP Office peut agir comme serveur de fichiers pour un maximum de 50 téléphones IP. Pour des quantités plus importantes, un serveur HTTP tiers distinct doit être utilisé.
<b>Responsable de passerelle H.323</b>	Le système IP Office exerce ce rôle.
<b>PC Manager</b>	Un PC fonctionnant sous Windows qui exécute IP Office Manager est requis pour apporter des modifications à la configuration d'IP Office. L'ordinateur doit également avoir System Status Application et System Monitor installés.
<b>Logiciel des téléphones IP</b>	Le logiciel d'installation du téléphone IP se trouve dans le dossier du programme de l'application IP Office Manager comme lors de l'installation des applications. Il est également fourni au cours de l'installation des applications IP Office Server Edition de l'application IP Office sur le serveur.
<b>Licences et abonnements</b>	Pour les systèmes qui ne fonctionnent pas en mode abonnement, chaque téléphone IP enregistré nécessite une licence. Sur les systèmes en mode abonnement, le poste doit être associé à un utilisateur abonné. Reportez-vous à la section Licences et abonnements.
<b>Serveur de sauvegarde/restauration</b>	Les téléphones sauvegardent et restaurent différents paramètres utilisateur et téléphone à chaque fois qu'un utilisateur se connecte ou se déconnecte. Pour ce faire, les fichiers stockés sur un serveur de fichiers sont utilisés. Il ne s'agit pas nécessairement du même serveur que celui utilisé pour les fichiers du firmware des téléphones. Le stockage de fichiers du système IP Office peut être utilisé pour cette fonction. Cette option est, par conséquent, recommandée.

## Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Licences et abonnements

### Abonnements

Les systèmes fonctionnant en mode abonnement prennent en charge les postes jusqu'au nombre total d'abonnements utilisateur disponibles.

### Licences

Pour les systèmes ne fonctionnant pas en mode abonnement, des licences sont requises pour chaque poste IP.

- Pour les systèmes IP Office Server Edition, un profil utilisateur doit être configuré pour les utilisateurs, avec une licence utilisateur telle que Basic User. Les utilisateurs sans licence ne peuvent pas se connecter à un poste.
- Les téléphones Avaya nécessitent chacun une licence de point d'extrémité IP Avaya. Cela concerne tous les téléphones des séries 1600, 9600, IP DECT, DECT R4 et Spectralink.
- Une licence de point d'extrémité IP tiers n'est requise que pour les téléphones IP qui ne sont pas des téléphones IP Avaya.
  - Les licences par défaut sont utilisées par chaque téléphone IP d'Avaya enregistré auprès du système IP Office dans l'ordre d'enregistrement. La licence redevient disponible si le téléphone annule son enregistrement. Toutefois, il est possible de réserver une licence pour certains téléphones afin d'être certain qu'ils disposent toujours d'une licence. Pour ce faire, il suffit de configurer **Réserver une licence de point d'extrémité Avaya IP** pour chaque poste IP. Pour les systèmes utilisant des licences WebLM, cette option est réglée sur Réserver une licence.
  - Les téléphones IP Avaya sans licence peuvent toujours enregistrer, mais sont limités aux appels d'urgence uniquement (codes courts d'urgence). L'utilisateur associé est alors considéré comme non connecté et le téléphone affiche « Aucune licence disponible ». Si une licence devient disponible, elle est tout d'abord assignée à n'importe quel combiné DECT ne disposant pas de licence, puis à n'importe quel autre téléphone Avaya sans licence afin de pouvoir enregistrer les téléphones.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

[Réservation des licences](#) à la page 37

---

## Évaluation du réseau

Le système IP Office est un véritable système Voice over IP (VoIP). Tous les postes téléphoniques et lignes réseau se connectent au système via le réseau de données des clients. Il est donc absolument impératif que le réseau du client soit évalué, puis reconfiguré si nécessaire, pour répondre aux besoins du trafic VoIP.

### Avertissement :

Lorsque vous installez des téléphones IP sur un système IP Office, Avaya suppose qu'une évaluation du réseau a été effectuée. Si un problème d'assistance remonte à Avaya, Avaya peut demander à voir les résultats d'une évaluation réseau récente et refuser d'apporter son aide si aucune évaluation satisfaisante n'a été réalisée.

La technologie actuelle permet de configurer les réseaux de manière optimale, et ainsi, d'obtenir des services VoIP d'une qualité vocale équivalente à celle du réseau public. Cependant, peu de réseaux sont configurés de manière optimale. C'est pourquoi il faut faire attention lors de l'évaluation de la qualité VoIP possible sur le réseau d'un client.

Tous les réseaux ne sont pas en mesure d'acheminer des transmissions vocales. Certains réseaux de données ne disposent pas d'une capacité suffisante ou ont des points de données ayant parfois un impact sur le trafic vocal. De plus, l'historique habituel de nombreux revendeurs concernant la croissance et le développement des réseaux de données via l'intégration de produits fait qu'il est nécessaire de tester tous les composants réseau pour confirmer leur compatibilité avec le trafic VoIP.

Une évaluation du réseau inclut les points suivants :

- Un audit du réseau pour examiner l'équipement existant et évaluer ses capacités, dont sa capacité à répondre aux besoins actuels et futurs en termes de voix et de données.
- Déterminer les objectifs du réseau, dont le type de trafic dominant, le choix des technologies et les paramètres des objectifs de qualité vocale.
- Cette évaluation devrait vous garantir que le réseau disposera de capacités suffisantes pour héberger le trafic de données et vocal prévu.

### **Cibles d'évaluation du réseau**

Les cibles de l'évaluation du réseau sont :

- Latence : inférieure à 180 ms pour une bonne qualité. Inférieure à 80 ms pour une qualité excellente. Il s'agit de la mesure de la durée de transfert du paquet dans un sens. Une plage de 80 ms à 180 ms est généralement acceptable. Veuillez noter que les différents codecs audio utilisés imposent chacun un délai fixe dû à la conversion du codec :
  - G.711 : 20 ms.
  - G.722 : 40 ms.
  - G.729 : 40 ms.
- Perte de paquets : inférieure à 3 % pour une bonne qualité. Inférieure à 1 % pour une qualité excellente. Une perte excessive de paquets sera audible : les mots sont coupés et on risque d'observer des retards de configuration de l'appel.
- Gigue : inférieure à 20 ms. La gigue est une mesure de la variance de la durée que mettent les différents paquets d'un même appel pour atteindre leur destination. Quand la gigue est trop importante, il y a de l'écho.
- Durée : statistiques à surveiller une fois par minute pendant une semaine complète. L'évaluation du réseau doit inclure les heures normales de fonctionnement.

### **Liens connexes**

[Téléphones IP H.323 IP Office](#) à la page 10

---

## **Canaux de compression de voix**

Les appels vers et depuis des appareils IP peuvent nécessiter d'être convertis vers le format du codec audio utilisé par l'appareil IP. Pour les systèmes IP Office, cette conversion est

effectuée par des canaux de compression de voix. Ceux-ci prennent en charge les formats codec audio IP communs G.711, G.722 et G.729a.

- Sur les unités de contrôle IP500 V2, vous pouvez ajouter des canaux en utilisant les cartes VCM IP500 et les cartes de combinaison IP500.
- Les systèmes IP Office Server Edition sont dotés d'un logiciel leur permettant de fournir leurs propres canaux de compression de voix, sans nécessiter de matériel supplémentaire.

Les canaux de compression de voix sont utilisés comme suit :

Type d'appel	Utilisation des canaux de compression de voix
<b>Appareil IP vers appareil non-IP</b>	Ces appels requièrent un canal de compression de voix pour la durée de l'appel. Si aucun canal n'est disponible, une indication d'occupation est retournée à l'appelant.
<b>Appareil IP vers appareil IP</b>	Les tonalités de progression d'appel (par exemple : tonalité de numérotation, tonalité secondaire de numérotation, etc.) ne requièrent pas de canaux de compression de voix avec les exceptions suivantes : <ul style="list-style-type: none"> <li>• Les tonalités de confirmation de code abrégé, d'ARS et saisie du code de compte ne requièrent pas de canal de compression de voix.</li> </ul> Lorsqu'un appel est connecté : <ul style="list-style-type: none"> <li>• Si les appareils IP utilisent le même codec audio, aucun canal de compression de voix n'est utilisé.</li> </ul> Si les appareils utilisent des codecs audio différents, un canal de compression de voix est requis pour chacun d'eux.
<b>Appareil non-IP vers appareil non-IP</b>	Aucun canal de compression de voix n'est requis.
<b>Musique d'attente</b>	Elle est fournie par le bus TDM d'IP Office et nécessite donc un canal de compression de voix lorsqu'elle est lue sur un périphérique IP.
<b>Ressources de conférence et appareils IP</b>	Les ressources de conférence sont gérées par la puce de conférence qui se trouve sur le bus TDM d'IP Office. Par conséquent, un canal de compression vocale est requis pour chaque périphérique IP utilisé dans la conférence. Ceci inclut les services qui utilisent des ressources de conférence telles l'écoute d'appel, l'intrusion, l'enregistrement d'appel et la surveillance silencieuse.
<b>Services de messagerie vocale et appareils IP</b>	Les appels vers les serveurs de messagerie vocale IP Office sont traités comme des appels de données du bus TDM. C'est pourquoi les appels provenant d'un périphérique IP vers une messagerie vocale nécessitent un canal de compression vocale.
<b>Appels fax</b>	Ceux-ci sont des appels vocaux avec une plage de fréquences légèrement plus large que les appels vocaux parlés. IP Office prend uniquement en charge le fax via IP entre les systèmes IP Office avec l'option Acheminement de fax sélectionnée. Il ne prend actuellement pas en charge T38.

*Le tableau continue ...*

Type d'appel	Utilisation des canaux de compression de voix
<b>Appels fax T38</b>	<p>IP Office 5.0 et les versions ultérieures prennent en charge les fax T38 sur les lignes de réseau et postes SIP. Chaque appel de fax T38 utilise un canal VCM.</p> <p>Dans un Small Community Network, un appel de télécopie T38 peut être converti en appel sur une ligne H.323 SCN à l'aide du protocole IP Office Support d'acheminement des télécopies. Cette conversion utilise 2 canaux VCM.</p> <p>Afin d'utiliser une connexion fax T38, la <b>Classification d'équipement</b> d'un poste analogique connecté à un fax peut être définie sur <b>Fax</b>. De plus, une nouvelle fonction de code court <b>Composer un numéro de fax</b> est disponible.</p>

**\* Remarque :**

les périphériques IP T3 doivent être configurés sur une taille de paquets de 20 ms pour que les conditions ci-dessus puissent s'appliquer. S'ils restent configurés pour une taille de paquets de 10ms, un canal de compression vocale est requis pour toutes les tonalités et pour les appels des médias non directs.

### Mesure de l'utilisation du canal

L'application System Status Application d'IP Office permet d'afficher l'utilisation des canaux de compression de voix. Dans la section Ressources, elle affiche le nombre de canaux en cours d'utilisation. Elle affiche également le nombre de fois où le nombre de canaux disponibles a été insuffisant et la dernière fois où un tel événement s'est produit.

Pour les cartes VCM IP500, le niveau d'utilisation des canaux est aussi indiqué par les voyants (1 à 8) situés à l'avant de la carte VCM IP500.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## QoS

Durant le transport de données vocales sur des liaisons à faible vitesse, il est possible que les paquets de données normaux (par exemple des paquets de 1 500 octets) empêchent ou retardent le passage des données vocales (en général 67 ou 31 octets) sur la liaison. Ce problème peut entraîner une qualité vocale médiocre.

Il est par conséquent vital que tous les routeurs et commutateurs du réseau disposent d'un mécanisme de qualité de service (QoS). Les routeurs QoS sont indispensables pour assurer une faible latence vocale et le maintien d'une qualité audio suffisante.

Le système IP Office prend en charge le mécanisme QoS de DiffServ (RFC2474). Celui-ci est basé sur le champ Type de service (ToS) dans l'en-tête de paquets IP. Sur les interfaces WAN, le système IP Office utilise ceci pour accorder la priorité aux voix et aux paquets de signalisation vocale. Les paquets vocaux volumineux sont également fragmentés, ce qui permet d'effectuer une compression d'en-tête VoIP (si celle-ci est prise en charge) afin de réduire le surdébit WAN.

**Liens connexes**

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Problèmes VoIP potentiels

Il est probable que toute erreur sur un réseau, indépendamment de sa cause, apparaisse initialement comme une dégradation de la qualité du fonctionnement VoIP. C'est le cas même si l'erreur n'est pas liée au matériel de téléphonie VoIP. Ainsi, en installant une solution VoIP, vous devez savoir que vous êtes le premier point de contact pour diagnostiquer et évaluer toutes les questions potentielles de réseau des clients.

	Description
<b>Normes de bout en bout correspondantes</b>	Le système VoIP dépend de la prise en charge et de la sélection de la même compression vocale, compression d'en-tête et des normes de qualité de service à tous les niveaux du routage des appels. Les points de démarrage et de fin doivent utiliser les mêmes méthodes de compression. Tous les points intermédiaires doivent prendre en charge la qualité de service Diff-Serv.
<b>Éviter les concentrateurs</b>	Les concentrateurs introduisent un écho ainsi que des points de congestion. Si le réseau du client nécessite des connexions LAN dépassant la capacité de l'unité IP Office, vous devez utiliser les commutateurs Ethernet. Même dans le cas contraire, les commutateurs Ethernet sont recommandés car ils autorisent la mise en oeuvre de la priorisation du trafic pour les périphériques VoIP.
<b>Conditionnement de l'alimentation, protection et sauvegarde</b>	Les systèmes téléphoniques traditionnels alimentent tous les appareils téléphoniques auxquels ils sont reliés depuis une source unique. Dans le cadre d'une installation VoIP, la même attention doit être accordée au conditionnement de l'alimentation, à la protection et à la sauvegarde sur le système téléphonique central que sur tous les périphériques du réseau IP.
<b>Multidiffusion</b>	Sur un réseau de données uniquement, il est possible qu'une imprimante ou qu'une carte de concentrateur mal installée multidiffuse du trafic sans que cette erreur soit immédiatement détectée. Sur un réseau VoIP, toute multidiffusion erronée affecte rapidement les appels et fonctions VoIP.
<b>Doublon d'adresses IP</b>	Les doublons d'adresses sont des problèmes fréquents.
<b>Utilisation excessive</b>	Une station de travail qui transmet constamment des niveaux de trafic élevés peut inonder un réseau et ainsi entraîner une panne du service VoIP.
<b>Accès au réseau</b>	Un réseau IP est beaucoup plus ouvert aux utilisateurs qui connectent de nouveaux appareils ou installent un logiciel sur des appareils existants ; ceux-ci ont alors un impact sur le système VoIP.
<b>Connexion de câbles</b>	Techniquement, le système VoIP peut (selon la largeur de bande) fonctionner sur toute connexion de réseau IP. En réalité, l'utilisation de câbles Cat5 est indispensable.

**Liens connexes**

[Téléphones IP H.323 IP Office](#) à la page 10

## Connexion au PC utilisateur

Afin de simplifier le nombre de connexions au réseau local depuis le bureau de l'utilisateur, il est possible d'acheminer le câble LAN Ethernet du PC via la plupart des téléphones IP Avaya.

Le câble LAN connecté au PC doit être relié au port identifié par le symbole PC (☐) sur la face arrière du téléphone IP. Il n'est pas nécessaire de modifier la configuration du réseau de l'ordinateur pour effectuer une connexion directe au réseau local. Ce port prend en charge les connexions Ethernet 10/100 Mbps. Les téléphones avec un suffixe G prennent également en charge les connexions 1000 Mbit/s.

Un adaptateur Gigabit (SAP 700416985) distinct doit être utilisé pour les téléphones non dotés d'un port pour PC. Ce périphérique sépare les données et la voix avant qu'elles n'atteignent le téléphone, pour fournir une sortie 10/100 mbit/s pour le téléphone et une sortie 10/100/1000 Mbit/s pour l'ordinateur. Cet adaptateur fonctionne sur l'alimentation du téléphone. Consultez les « *instructions de sécurité et d'installation de l'adaptateur Gigabit Ethernet* » (16-601543).

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

## Options d'alimentation

Chaque téléphone H.323 nécessite une alimentation. Il ne s'alimente pas sur le système téléphonique. Les options d'alimentation possibles sont énumérées ci-après.

IEEE 802.3af correspond à une norme couramment appelée Alimentation sur Ethernet (PoE). Elle permet aux périphériques de réseau d'être alimentés via le câble de réseau à l'aide des mêmes câbles que ceux des signaux de données. Tous les téléphones IP H.323 d'Avaya pris en charge sur le système IP Office prennent également en charge cette norme.

Si une quantité importante de téléphones est installée, l'utilisation de commutateurs PoE est recommandée. Pour les autres scénarios, des périphériques à injecteur PoE distincts peuvent être utilisés pour ajouter la prise en charge de l'alimentation PoE à la connexion LAN du téléphone à partir d'un commutateur autre que PoE.

Téléphones IP H.323	Modèles pris en charge	Classe PoE 802.3af	
		PoE	Inactif
Série 1600	1603	2	4,4 W
	1603W	2	4,4 W
	1608	2	3,7 W
	1616	2	2,7 W
Série 9600	9608	1	2,08 W
	9611G	1	2,8 W
	9621G	2	3,49 W
	9641G	2	3,44 W

Ces téléphones des séries 1603 et 1603SW nécessitent un séparateur d'alimentation PoE distinct pour être alimentés de cette manière.

Le dépassement de la limite de classe d'un port PoE ou du maximum pris en charge par une classe de commutateur PoE peut entraîner des dysfonctionnements.

Veillez noter que pour les téléphones utilisés avec un module de boutons complémentaire et d'autres accessoires, les besoins en alimentation sont plus élevés. Pour les téléphones 9608, 9611, 9621 et 9641, configurez le commutateur d'alimentation sur H et considérez le téléphone comme faisant partie de la Classe 3.

### **Téléphones de la série 1600**

Ces téléphones peuvent utiliser l'alimentation sur Internet (PoE) comme décrit précédemment ou être alimentés par l'utilisation d'unités d'alimentation (PSU) de la série 1600. Différents modèles d'unités d'alimentation (PSU) existent pour chaque type de prise secteur selon les pays. L'unité d'alimentation (PSU) se connecte au téléphone à l'aide d'un connecteur annulaire situé sous le téléphone.

### **Téléphones 9608, 9611, 9621 et 9641**

Ces téléphones prennent uniquement en charge un câble d'alimentation par Ethernet (PoE). S'il n'est pas fourni par un commutateur PoE, il est alors possible d'utiliser un injecteur PoE à port unique Avaya distinct pour chaque téléphone.

#### **Liens connexes**

[Téléphones IP H.323 IP Office](#) à la page 10

---

## **Options du serveur de fichiers**

Au cours des phases d'installation et de maintenance, les téléphones téléchargent différents fichiers du firmware. Pour ce faire, le téléphone demande d'abord les fichiers auprès d'un serveur HTTPS. S'il n'obtient pas de réponse, il tente à nouveau d'obtenir les fichiers auprès d'un serveur HTTP. L'adresse du serveur à utiliser est fournie dans la réponse DHCP que le téléphone a reçue de la part du serveur DHCP. Si le système IP Office est utilisé comme serveur DHCP, l'adresse du serveur de fichiers est définie dans configuration d'IP Office. Pour les téléphones installés en utilisant l'adressage statique, l'adresse du serveur de fichiers est l'une des adresses saisies lors de l'installation.

- Chaque téléphone tente de demander des fichiers provenant du serveur de fichiers à chaque fois qu'il est redémarré. Toutefois, si le téléphone ne reçoit pas de réponse, il continue à redémarrer en utilisant les fichiers existants contenus dans sa mémoire. Par conséquent, il n'est pas obligatoire que le serveur de fichiers soit disponible en permanence après l'installation initiale.
- Les téléphones utilisent également un serveur pour la sauvegarde et la restauration des paramètres utilisateur pendant le fonctionnement du téléphone. L'adresse de ce serveur est déterminée par une adresse séparée définie qui figure dans le fichier `46xxsettings.txt`. Il ne s'agit pas nécessairement du même serveur que celui utilisé pour le micrologiciel du téléphone. Toutefois, pour le fonctionnement d'IP Office, l'adresse du serveur IP Office est recommandée pour une utilisation comme serveur de fichiers de sauvegarde/restauration.

Les options suivantes sont disponibles pour le serveur de fichiers des téléphones IP installés sur un système IP Office.

Serveur de fichiers	X téléphones maximum	TFTP (Port 69)	HTTP (Port 80)	HTTPS (Port 411)
IP Office Manager Lorsqu'il est exécuté, IP Office Manager peut jouer le rôle de serveur HTTP / TFTP pour les requêtes de fichiers des téléphones IP.	5	✓	✓	-
Carte mémoire IP500 V2 Pour les unités de contrôle IP Office dotées d'une carte mémoire, cette dernière peut être utilisée pour fournir les fichiers logiciels. Pour les unités de contrôle IP500 V2, la carte SD du système est un élément obligatoire et est préchargée avec les fichiers du micrologiciel du téléphone pendant la création et les mises à niveau de la carte. Divers autres fichiers peuvent être générés automatiquement par IP Office s'ils ne sont pas présents sur la carte mémoire.	50	✓	✓	✓
IP Office Server Edition/IP Office Select Pour les systèmes IP Office, l'application IP Office peut servir de serveur de fichiers. Les fichiers du micrologiciel du téléphone sont installés sur le serveur dans le cadre de l'installation d'IP Office. Divers autres fichiers peuvent être générés automatiquement par IP Office s'ils ne sont pas présents sur la carte mémoire.	1	-	✓	✓
Logiciel tiers Le logiciel du serveur de fichiers HTTP/TFTP tiers est disponible auprès de nombreuses sources, et notamment d'Avaya.	-	✓	✓	✓

<sup>1</sup> Dans un réseau IP Office Server Edition/IP Office Select, les serveurs (autres qu'une extension IP500 V2) peuvent servir de serveur de fichiers pour la capacité totale des systèmes des téléphones. Toutefois, le taux de prise en charge de la mise à jour du micro-logiciel dépend du type de serveur comme suit. Si des performances de mise à niveau supérieures à ces chiffres sont requises, un serveur de fichiers HTTP/S externe peut être utilisé.

- Dell R240 : 100 téléphones en 50 minutes.
- HP DL360G7 : 200 téléphones en 50 minutes.
- Dell R240 : 300 téléphones en 50 minutes.
- OVA : jusqu'à 300 téléphones en 50 minutes.

<sup>2</sup> Pour les systèmes IP Office version 9.0 utilisés comme serveurs de fichiers, la redirection HTTP peut être appliquée afin de rediriger les requêtes de fichiers .bin des téléphones 9608, 9611, 9621 et 9641 vers un serveur HTTP séparé.

## Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Cartes mémoire de l'unité de contrôle

La carte mémoire utilisée avec les systèmes IP500 V2 peut être utilisée pour stocker des fichiers, y compris ceux utilisés par les téléphones IP d'Avaya.

L'unité de contrôle IP500 V2 nécessite toujours une carte SD système. Lors de la création de cette carte, un ensemble complet de fichiers de micrologiciel IP Office, y compris ceux utilisés par les téléphones IP d'Avaya, est placé sur la carte.

### Test du serveur de fichiers

Vous pouvez utiliser un navigateur Web pour effectuer un test basique du serveur de fichiers. Par exemple, si vous utilisez HTTP, la saisie de `http://<server_address>/46xxsettings.txt` doit afficher le fichier `46xxsettings.txt`.

Si vous utilisez le système IP Office pour générer automatiquement des fichiers, le fichier de paramètres comprend du texte indiquant qu'il a été généré automatiquement par le système en réponse à la demande de fichier. Ceci est utile, non seulement pour vérifier le fonctionnement du serveur de fichiers, mais également pour voir les paramètres fournis par le système IP Office.

## Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Demandes de fichiers du téléphone

Au démarrage, la plupart des téléphones IP Avaya suivent un processus de demande de plusieurs fichiers auprès d'un serveur de fichiers :

1. En général, cette procédure commence par la demande d'un fichier de mise à niveau. Ce fichier indiquera quel micro-logiciel le téléphone doit exécuter. Si celui-ci est différent du micro-logiciel actuel, les fichiers logiciels listés seront ajoutés à la liste des téléchargements. La dernière ligne du fichier de mise à niveau indique au téléphone quel est le nom du fichier de paramètres qu'il doit demander.
2. Le téléphone demande un fichier de paramètres. Ce fichier transmet la majeure partie des paramètres de configuration au téléphone. Il peut également contenir une liste de fichiers supplémentaires que le téléphone doit demander, comme les fichiers de langue et les économiseurs d'écran.
3. Le téléphone demande les fichiers supplémentaires :
  - Tous les fichiers du micro-logiciel signalés par le fichier de mise à niveau ;
  - Tous les fichiers supplémentaires signalés par le fichier de paramètres ;
  - Tous les fichiers de paramètres supplémentaires.
4. Le téléphone peut également demander un fichier de paramètres de l'utilisateur.

La liste ci-dessus n'est qu'un résumé. En fonction du téléphone, la liste des fichiers demandés peut varier. Par ailleurs, si le téléphone demande un micro-logiciel pour une mise à niveau, il est susceptible de ne pas demander d'autres fichiers tant que la mise à niveau du micro-logiciel ne sera pas terminée et que l'appareil n'aura pas été redémarré.

Lorsque le système IP Office est utilisé comme serveur de fichiers, il a la possibilité de générer automatiquement la plupart des fichiers demandés par le téléphone.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

[Génération automatique du fichier](#) à la page 27

---

## Génération automatique du fichier

Les téléphones IP Avaya demandent plusieurs fichiers au serveur de fichiers lorsque le téléphone redémarre. Par exemple, des fichiers du micrologiciel et de configuration du téléphone.

Lorsque le système IP Office est utilisé en tant que serveur de fichiers et que le téléphone demande un fichier, si ce dernier n'est pas disponible, le système peut en générer un automatiquement. Le fichier généré automatiquement utilisera une combinaison de paramètres et d'options par défaut de la configuration du système. Une fois soumis au téléphone demandant, le fichier généré automatiquement n'est pas conservé sur le système.

Cette fonction est utilisée pour la plupart des types de fichiers, sauf pour les fichiers réels du micrologiciel (par exemple, .bin, .zip, .tar) et les fichiers de certificat. Si un fichier réel est chargé sur le système, la génération automatique de ce fichier particulier s'arrête.

Dans le fichier `46xxsettings.txt` généré automatiquement :

- Les paramètres reposant sur les entrées de configuration IP Office (par exemple, les paramètres de langue) apparaissent dans la section intitulée `AUTOGENERATEDSETTINGS`.
- Les paramètres qui restent les mêmes pour tous les systèmes IP Office utilisant la même version du logiciel apparaissent dans la section intitulée `NONAUTOGENERATEDSETTINGS`.

### Test du serveur de fichiers

Vous pouvez utiliser un navigateur Web pour effectuer un test basique du serveur de fichiers. Par exemple, si vous utilisez HTTP, la saisie de `http://<server_address>/46xxsettings.txt` doit afficher le fichier `46xxsettings.txt`.

Si vous utilisez le système IP Office pour générer automatiquement des fichiers, le fichier de paramètres comprend du texte indiquant qu'il a été généré automatiquement par le système en réponse à la demande de fichier. Ceci est utile, non seulement pour vérifier le fonctionnement du serveur de fichiers, mais également pour voir les paramètres fournis par le système IP Office.

### Liens connexes

[Demandes de fichiers du téléphone](#) à la page 26

---

## Carte mémoire de l'unité de contrôle

La carte mémoire utilisée avec les systèmes IP500 V2 peut être utilisée pour stocker des fichiers, y compris ceux utilisés par les téléphones IP d'Avaya.

L'unité de contrôle IP500 V2 nécessite toujours une carte SD système. Lors de la création de cette carte à l'aide d'IP Office Manager, un ensemble complet de fichiers de micrologiciel IP Office, y compris ceux utilisés par les téléphones IP d'Avaya, est placé sur la carte.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Mise sur liste noire des enregistrements

Le système IP Office enregistre les demandes d'enregistrement H323/SIP ayant fait l'objet d'un échec. Plusieurs tentatives échouées peuvent entraîner le blocage pendant un certain temps de l'extension et/ou de l'adresse IP.

Le blocage s'applique comme suit :

Méthode	Description
<b>Blocage du poste</b>	Les tentatives d'enregistrement à un poste existant à l'aide d'un mauvais mot de passe sont bloquées pendant 10 minutes après 5 tentatives échouées sur une période de 10 minutes.
<b>Blocage de l'adresse IP</b>	Les tentatives d'enregistrement à un poste non existant ou à l'aide d'un mauvais mot de passe pour un poste existant sont bloquées pendant 10 minutes après 10 tentatives échouées sur une période de 10 minutes.

Lorsque le blocage se produit, le système génère une alerte dans System Status Application et ajoute une entrée à son journal d'audit. Une alerte système est également générée et peut être produite à l'aide de n'importe quel itinéraire d'alerte du système pris en charge (SMTP, SNMP, Syslog).

System Monitor peut afficher les détails des adresses IP et des postes sur liste noire. Sélectionnez **État > Adresses IP et statut sur liste noire > Postes sur liste noire**.

### Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

---

## Blocage des codes d'accès par défaut

### À propos de cette tâche

Pour IP Office 11.0 et les versions supérieures, les paramètres de sécurité par défaut bloquent l'utilisation de mots de passe par défaut tels que 0000 pour l'enregistrement des postes.

## Procédure

1. En utilisant IP Office Manager, accédez à la configuration de sécurité du système.
2. Dans l'onglet **Général**, décochez la case **Bloquer les codes d'accès du téléphone IP par défaut**.
3. Enregistrez les paramètres.

## Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

# Chapitre 2 : Paramètres supplémentaires du téléphone

Les fichiers de paramètres `46xxsettings.txt` générés automatiquement conviennent pour la plupart des installations. En revanche, dans certains cas, il peut être nécessaire de modifier la valeur des paramètres du fichier ou d'ajouter d'autres paramètres. Vous avez différentes manières d'y parvenir :

- **À l'aide de fichiers statiques** : remplacez le fichier généré automatiquement par un fichier réel. Cette méthode est recommandée uniquement pour les personnes ayant l'habitude de modifier les fichiers de paramètres des téléphones Avaya. Le principal inconvénient, c'est que vous ne profiterez plus de la modification automatique des paramètres afin qu'ils correspondent aux modifications apportées à la configuration IP Office. Reportez-vous à la section [Configuration et modification des paramètres des fichiers](#) à la page 33.
- **À l'aide d'un fichier de paramètres** : si un fichier nommé `46xxsettings.txt` se trouve dans le système, le fichier `46xxsettings.txt` généré automatiquement invite le téléphone à demander ce fichier. Cela vous permet de télécharger un fichier spécial contenant les paramètres supplémentaires ou les paramètres modifiés dans le fichier généré automatiquement. Reportez-vous à la section [46xxspecials.txt](#) à la page 31.
- **À l'aide des numéros source Aucun utilisateur** : vous pouvez utiliser plusieurs paramètres Numéro source Aucun utilisateur pour ajouter des valeurs spéciales au fichier de paramètres généré automatiquement. Reportez-vous à la section [NoUser Source Numbers](#) à la page 32.

## Commandes supplémentaires courantes

Les commandes supplémentaires suivantes font partie des plus courantes. Pour plus d'informations sur les commandes disponibles, consultez le manuel de l'administrateur Avaya portant sur cette série de téléphones.

Description	Commande du fichier de paramètres
<b>Mot de passe/CRAFT</b> Définissez le PROCPSWD spécifié dans le fichier <code>46xxsettings.txt</code> créé automatiquement, où X correspond au mot de passe. Cette procédure est utile pour l'utilisation de TLS, qu'il n'est pas possible d'activer sur les téléphones avec le PROCPSWD par défaut.	SET PROCPSWD X

*Le tableau continue ...*

Description	Commande du fichier de paramètres
<p><b>Mot de passe de l'administrateur</b></p> <p>Définissez le mot de passe administrateur du téléphone Vantage spécifié dans le fichier <code>46xxsettings.txt</code> généré automatiquement, où X correspond au mot de passe.</p>	SET ADMIN_PASSWORD X
<p><b>Fonctionnement du casque</b></p> <p>Par défaut, le casque du téléphone est raccroché lorsque l'intervenant se déconnecte. La définition de ce numéro source modifie cette action par défaut. Le casque n'est pas raccroché lorsque l'intervenant se déconnecte.</p>	SET HEADSYS 1
<p><b>Délai de rétroéclairage</b></p> <p>Indique le délai de rétroéclairage du téléphone (en minutes).</p>	SET BAKLIGHTOFF 60
<p><b>Économiseur d'écran</b></p> <p>Les commandes suivantes permettent :</p> <ol style="list-style-type: none"> <li>1. d'activer l'économiseur d'écran ;</li> <li>2. de définir le nom de l'économiseur d'écran à télécharger ;</li> <li>3. de définir le nom du fichier téléchargé à utiliser.</li> </ol>	SET SCREENSAVERON SET SCREENSAVER_IMAGE J179scr_svr.jpg SET SCREENSAVER_IMA- GE_DISPLAY J179scr_svr
<p><b>Image d'arrière-plan</b></p> <p>Les commandes suivantes permettent :</p> <ol style="list-style-type: none"> <li>1. de définir le nom de l'image d'arrière-plan à télécharger ;</li> <li>2. d'indiquer le nom du fichier téléchargé à utiliser.</li> </ol>	SET BACKGROUND_IMAGE J179bck_grnd.jpg SET BACKGROUND_IMA- GE_DISPLAY J179bck_grnd

Il existe plusieurs numéros source Aucun utilisateur pour les extensions distantes. Ils fonctionnent différemment dans la mesure où ils modifient les valeurs existantes attribuées à un téléphone dans le fichier de paramètres généré automatiquement lorsque le système détecte que le téléphone demandant le fichier est un poste distant. Référez-vous au manuel « *Téléphones SIP IP Office avec ABSCE* ».

### Liens connexes

[46xxspecials.txt](#) à la page 31

[NoUser Source Numbers](#) à la page 32

[Configuration et modification des paramètres des fichiers](#) à la page 33

---

## 46xxspecials.txt

Pour les systèmes utilisant le fichier `46xxsettings.txt` généré automatiquement, il est possible d'ajouter des paramètres supplémentaires manuellement via un fichier appelé `46xxspecials.txt`. Lorsque ce fichier est ajouté au système, la commande **GET 46xxspecials.txt** apparaît sur la dernière ligne du fichier `46xxspecials.txt` généré automatiquement et demandé par les téléphones.

Le fichier `46xxspecials.txt` doit être créé manuellement, puis placé sur le serveur de fichiers du téléphone. Il peut s'agir d'un :

- Simple fichier texte comprenant une seule commande.
- Fichier de paramètres complexe comprenant des paramètres en fonction du type de téléphone, du modèle et/ou du groupe.

Pour obtenir un exemple de structure complexe, vous pouvez vous rendre à l'adresse <http://<IPOffice>/46xxspecials.txt> pour télécharger un fichier généré automatiquement. Sauvegardez et modifiez ce fichier avant de le charger sur le système.

## Liens connexes

[Paramètres supplémentaires du téléphone](#) à la page 30

---

## NoUser Source Numbers

Most values in the auto-generated settings file are based on settings taken from the IP Office system configuration. However, it may occasionally be necessary to add additional values to the auto-generated files. This can be done using the values entered as `NoUser` source numbers.

- Since these changes are applied to the values in the auto-generated `46xxsettings.txt` file, they are overridden by any setting entered in the `46xxsettings.txt` file if present.
- There are a number of **Aucun utilisateur** source number settings used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. Refer to the [IP Office SIP Phones with ASBCE](#) manual.

### Example NoUser Source Numbers

	Description
<code>SET_46xx_PROCPSWD=X</code>	This NoUser source number adds the command <code>SET PROCPSWD X</code> to the auto-generated settings file where <code>X</code> is the password set.
<code>SET_ADMINPSWD=X</code>	This NoUser source number adds the command <code>SET ADMINPSWD X</code> to the auto-generated settings file where <code>X</code> is the password set.
<code>SET_HEADSYS_1</code>	This NoUser source number adds the command <code>SET ADMINPSWD X</code> to the auto-generated settings file.
<code>SET_BAKLIGHTOFF=N</code>	This NoUser source number adds the command <code>SET BAKLIGHTOFF N</code> to the auto-generated settings file provided to a remote extension. <code>N</code> is the timeout in minutes.

## Related links

[Paramètres supplémentaires du téléphone](#) on page 30

# Configuration et modification des paramètres des fichiers

## À propos de cette tâche

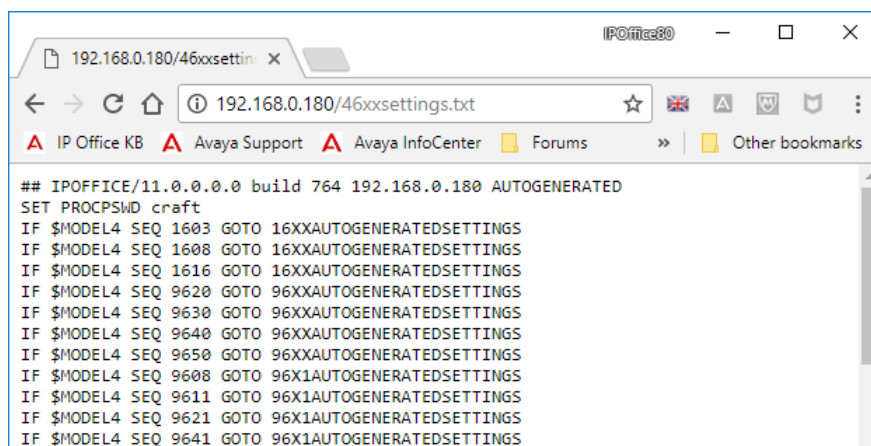
La plupart des téléphones IP Avaya téléchargent un fichier de paramètres lorsqu'ils sont redémarrés. Ce fichier contient un éventail de paramètres.

### \* Remarque :

Lorsque vous le pouvez, utilisez le système IP Office en tant que serveur de fichiers et laissez-le générer automatiquement les fichiers de paramètres. Cela permet au système de régler automatiquement les paramètres fournis aux téléphones afin qu'ils correspondent aux modifications apportées au niveau de la configuration du système.

## Procédure

1. Naviguez vers le système et saisissez le nom du fichier de paramètres du téléphone requis, par exemple <http://192.168.42.1/46xxsettings.txt>. Le fichier généré automatiquement est affiché dans le navigateur.



```

## IPOFFICE/11.0.0.0.0 build 764 192.168.0.180 AUTOGENERATED
SET PROCPSWD craft
IF $MODEL4 SEQ 1603 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1608 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1616 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9620 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9630 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9640 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9650 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9608 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9641 GOTO 96X1AUTOGENERATEDSETTINGS

```

- La plupart des téléphones : 46xxsettings.txt
  - Série 1100/1200 : 11xxsettings.txt
  - H175 : H1xxsettings.txt
2. Enregistrez le fichier en tant que fichier texte local.
    - Pour enregistrer le fichier à partir du navigateur Chrome, cliquez avec le bouton droit sur la fenêtre et sélectionnez **Enregistrer sous**.
    - Pour enregistrer le fichier à partir du navigateur Explorer, sélectionnez **Fichier > Enregistrer sous**.
    - Pour enregistrer le fichier à partir du navigateur Firefox, sélectionnez **Enregistrer la page sous**.

Le fichier téléchargé peut à présent être modifié à l'aide d'un éditeur de texte. Les champs pris en charge sont décrits dans le manuel d'administration adapté à la série de téléphones.

3. Une fois terminé, chargez le fichier sur le serveur de fichiers utilisé par les téléphones.

## Paramètres supplémentaires du téléphone

4. Redémarrez le(s) téléphone(s) pour recharger les fichiers et télécharger le fichier de paramètres modifié.

### Liens connexes

[Paramètres supplémentaires du téléphone](#) à la page 30

# Partie 2 : Processus d'installation de base

## Installation du téléphone IP H.323

Vous trouverez ci-après un résumé des principales étapes de la procédure d'installation. La méthode d'installation recommandée consiste à utiliser, si possible, le serveur DHCP, afin de se servir du système IP Office comme serveur de fichiers et d'activer la création automatique d'utilisateurs et de postes.

	Description
<b>PC Manager :</b>	Vérifiez qu'IP Office Manager, System Status Application et System Monitor sont installés et peuvent être utilisés pour se connecter au système IP Office. Vérifiez que vous pouvez recevoir la configuration provenant du système et la renvoyer.
<b>Canaux de compression de voix</b>	Sur les systèmes IP500 V2, l'unité de contrôle doit être équipée de canaux de compression de voix. Utilisez l'application System Status Application (SSA) ou System Monitor pour vérifier que les canaux de compression de voix sont disponibles. SSA répertorie les canaux des modules de compression de voix (VCM) sur l'écran <b>Ressources</b> . Les premières lignes de sortie de Monitor comprennent l'élément VCOMP= qui indique le nombre de canaux VCM installés sur l'unité de contrôle.
<b>Licences ou abonnements</b>	Selon le mode de fonctionnement du système, chaque téléphone nécessite une licence ou un abonnement. Les téléphones sans licence ni abonnement pourront toujours être enregistrés, mais ne fonctionneront pas. Reportez-vous à la section <a href="#">Licences et abonnements</a> à la page 18.
<b>Paramètres du responsable de passerelle H.323</b>	La prise en charge des téléphones H.323 est activée par défaut dans le système IP Office. Cependant, le paramètre doit être vérifié.
<b>Paramètre du serveur DHCP</b>	Nous recommandons d'utiliser le DHCP pour installer des téléphones IP sur un système IP Office. Cette méthode requiert qu'un serveur DHCP soit configuré pour prendre en charge les téléphones IP. Pour ce faire, le système IP Office peut être utilisé. Si le client souhaite utiliser son propre serveur DHCP, une configuration supplémentaire est nécessaire.

*Le tableau continue ...*

	Description
<b>Paramètre du serveur de fichiers des téléphones</b>	Si le système IP Office est utilisé pour le serveur DHCP, il doit également être configuré avec l'adresse du serveur de fichiers. Quels que soient la méthode d'installation et le serveur de fichiers sélectionnés, les fichiers du micrologiciel du téléphone doivent être ajoutés aux fichiers disponibles sur le serveur.
<b>Paramètres des postes et utilisateurs</b>	Le système IP Office peut être configuré pour créer automatiquement des entrées utilisateur et poste dans sa configuration pour chaque téléphone IP installé. Si la création automatique n'est pas utilisée, les entrées doivent être créées manuellement pour chaque poste et utilisateur avant l'installation des téléphones.
<b>Connexion des téléphones</b>	Une fois les étapes décrites ci-dessus terminées, les téléphones peuvent être connectés au réseau. Si vous utilisez un serveur DHCP, les téléphones obtiennent automatiquement des informations relatives à l'adresse IP et à d'autres paramètres, puis commencent à charger les fichiers. Si le serveur DHCP n'est pas utilisé, il n'est pas nécessaire que les téléphones suivent une procédure manuelle de saisie des informations relatives à l'adresse IP et des paramètres.
<b>Enregistrement du téléphone</b>	Une fois que les téléphones ont téléchargé tous les fichiers dont ils ont besoin sur le serveur de fichiers, ils tentent de s'enregistrer avec le système IP Office. Les téléphones demandent une saisie du numéro de poste qu'ils devront utiliser.
<b>Test</b>	Le fonctionnement des téléphones doit être testé en passant quelques appels, et notamment des appels externes.
<b>Après l'installation</b>	Si la fonction de création automatique a été utilisée pour des postes ou des utilisateurs, ces paramètres doivent être désactivés une fois l'installation de tous les téléphones terminée. Ce manuel détaille uniquement la configuration utilisateur minimale requise pour l'installation. Les nouveaux utilisateurs peuvent désormais être complètement configurés pour répondre aux besoins de ces utilisateurs.

# Chapitre 3 : Licences et abonnements

## Abonnements

Les systèmes fonctionnant en mode abonnement prennent en charge les postes jusqu'au nombre total d'abonnements utilisateur disponibles.

## Licences

Pour les systèmes ne fonctionnant pas en mode abonnement, des licences sont requises pour chaque poste IP.

- Pour les systèmes IP Office Server Edition, un profil utilisateur doit être configuré pour les utilisateurs, avec une licence utilisateur telle que Basic User. Les utilisateurs sans licence ne peuvent pas se connecter à un poste.
- Les téléphones Avaya nécessitent chacun une licence de point d'extrémité IP Avaya. Cela concerne tous les téléphones des séries 1600, 9600, IP DECT, DECT R4 et Spectralink.
- Une licence de point d'extrémité IP tiers n'est requise que pour les téléphones IP qui ne sont pas des téléphones IP Avaya.
  - Les licences par défaut sont utilisées par chaque téléphone IP d'Avaya enregistré auprès du système IP Office dans l'ordre d'enregistrement. La licence redevient disponible si le téléphone annule son enregistrement. Toutefois, il est possible de réserver une licence pour certains téléphones afin d'être certain qu'ils disposent toujours d'une licence. Pour ce faire, il suffit de configurer **Réserver une licence de point d'extrémité Avaya IP** pour chaque poste IP. Pour les systèmes utilisant des licences WebLM, cette option est réglée sur Réserver une licence.
  - Les téléphones IP Avaya sans licence peuvent toujours enregistrer, mais sont limités aux appels d'urgence uniquement (codes courts d'urgence). L'utilisateur associé est alors considéré comme non connecté et le téléphone affiche « Aucune licence disponible ». Si une licence devient disponible, elle est tout d'abord assignée à n'importe quel combiné DECT ne disposant pas de licence, puis à n'importe quel autre téléphone Avaya sans licence afin de pouvoir enregistrer les téléphones.

## Liens connexes

[Téléphones IP H.323 IP Office](#) à la page 10

[Réserve des licences](#) à la page 37

---

## Réserve des licences

### À propos de cette tâche


Cette procédure particulière peut généralement être suivie jusqu'à ce que le poste soit créé. Si la fonction de création de poste automatique (par défaut) est utilisée, cela signifie que la réserve des licences ne pourra avoir lieu qu'après l'installation initiale du téléphone. Toutefois, une attention toute particulière doit être accordée dans l'utilisation de ce paramètre

avec des téléphones déjà installés, afin de s'assurer qu'ils conservent bien leurs licences, si possible, suite à l'ajout d'autres téléphones.

Généralement, les licences sont automatiquement affectées aux extensions dans l'ordre d'enregistrement. Cependant, les numéros de postes existant peuvent réserver une licence afin de s'assurer qu'elles restent valides lorsque de nouveaux numéros de postes ajoutés au système parviennent à s'enregistrer juste après un redémarrage du système.

- Pour les systèmes utilisant des licences WebLM, cette option est réglée sur Réserver une licence.
- La réservation des licences n'est pas prise en charge sur les systèmes en mode abonnement.

### Procédure

1. Utilisez IP Office Manager, pour recevoir la configuration du système téléphonique.
2. Sélectionnez  **Poste** , puis le poste H.323.
3. Sélectionnez l'onglet **VoIP**.
4. Définissez le champ **Réserver une licence** sur **Réserver une licence de point d'extrémité Avaya IP**.
5. Reproduisez la procédure pour tous les autres numéros de postes pour lesquels vous souhaitez réserver une licence.
6. Enregistrez la configuration.

### Liens connexes

[Licences et abonnements](#) à la page 18

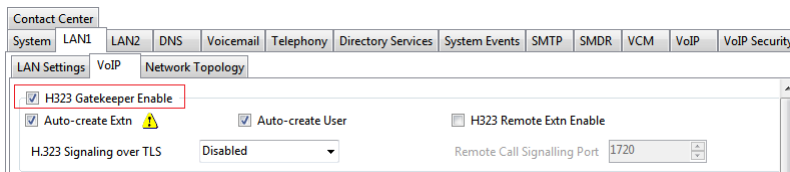
# Chapitre 4 : Activation du responsable de passerelle H.323

## À propos de cette tâche

La prise en charge des téléphones et lignes H.323 est activée par défaut. Cependant, les paramètres doivent être vérifiés.

## Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez **Système**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. Sélectionnez le sous-onglet **VoIP**.



5. Cochez la case du paramètre **Activer le responsable de passerelle H.323**.
6. Enregistrez la configuration.

## Liens connexes

[Configuration de la plage de ports RTP](#) à la page 39

[Paramétrage de la qualité de service \(QoS\) de DiffServ](#) à la page 41

[Codecs par défaut du système](#) à la page 41

---

## Configuration de la plage de ports RTP

### À propos de cette tâche


Les ports utilisés pour les appels VoIP H.323 varient pour chaque appel. La plage des ports utilisés peut être ajustée afin d'éviter tout conflit avec les autres services. Si le client dispose de pare-feux internes ou d'équipements similaires qui s'appliquent au filtrage des ports ou n'acheminent que le trafic basé sur le port utilisé, la plage configurée ici doit être autorisée par ces périphériques.

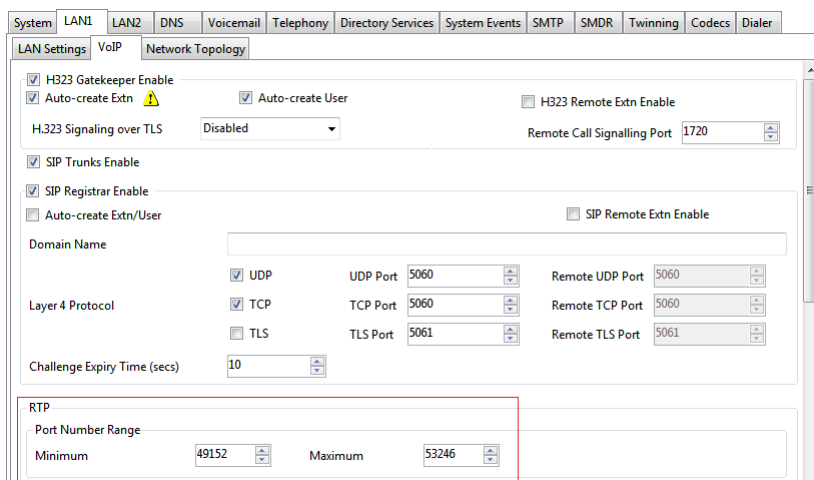
Pour chaque appel VoIP, les ports de réception sont sélectionnés dans la plage définie ci-dessous. Les numéros pairs de la plage sont utilisés pour le trafic Real-Time Transport

Protocol (RTP) entrant des appels. Ce même trafic Real-Time Transport Control Protocol (RTCP) d'appels utilise le numéro de port RTP plus 1, c'est-à-dire les numéros impairs.

Il est conseillé d'utiliser uniquement les numéros de port égaux ou supérieurs à 49152 mais strictement inférieurs à 65535, ce qui correspond à la plage définie par l'IANA (Autorité d'Affectation de Numéros sur Internet), dans le cadre d'une utilisation dynamique.

## Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. Sélectionnez le sous-onglet **VoIP**.



5. Vérifiez la **Plage de numéros de ports** indiquée dans la section **RTP**. N'oubliez pas que le trafic RTCP correspondant utilise la même plage plus 1.

- **Minimum** : par défaut = 49152. Plage = 1024 à 65280.

Celle-ci définit la limite inférieure des numéros de port RTP qu'utilise le système. Le choix d'une plage minimum inférieure à 1024 doit uniquement se faire après une analyse minutieuse de l'ensemble de la configuration.

- **Maximum** : par défaut = 53246. Plage = 1278 à 65534.

Elle définit la limite supérieure des numéros de port RTP qu'utilise le système. L'écart entre les plages minimum et maximum doit être d'au moins 254. Le choix d'une plage minimum inférieure à 1024 doit uniquement se faire après une analyse minutieuse de l'ensemble de la configuration.

6. Enregistrez la configuration.

## Liens connexes

[Activation du responsable de passerelle H.323](#) à la page 39


## Paramétrage de la qualité de service (QoS) de DiffServ

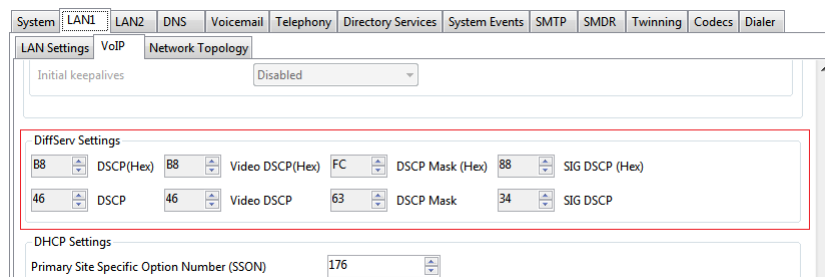
### À propos de cette tâche

DiffServ est utilisé pour appliquer différentes balises de « qualité de service » aux éléments voix (RTP) et signaux de commande (RTCP) d'un appel VoIP. Le système IP Office n'applique pas de lui-même une priorité différente aux paquets de données qu'il reçoit ou envoie en fonction de leurs balises. Toutefois, lorsqu'il est utilisé dans un réseau où la qualité de service (QoS) est utilisée pour hiérarchiser les priorités par les autres périphériques, les paramètres d'IP Office doivent être configurés pour correspondre à ceux prévus pour les appels vocaux et les signaux de commande qui y sont associés.

signalling.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. Sélectionnez le sous-onglet **VoIP**.



Vérifiez les **Paramètres DiffServ** utilisés par le système. Notez que les deux lignes sont reliées. La ligne supérieure indique les valeurs DiffServ sous forme de chiffres hexadécimaux et la ligne inférieure, les valeurs sous forme de décimales. Les valeurs hexadécimales équivalent à la décimale multipliée par 4. L'une ou l'autre ligne peut être utilisée pour configurer les valeurs requises.

5. Enregistrez la configuration.

### Liens connexes

[Activation du responsable de passerelle H.323](#) à la page 39


## Codecs par défaut du système

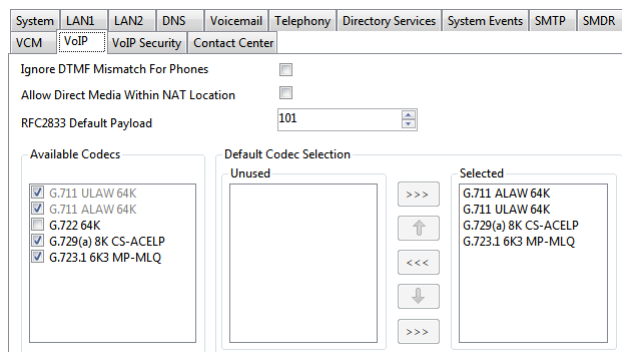
### À propos de cette tâche

Par défaut, tous les périphériques VoIP ajoutés à la configuration d'IP Office utilisent les préférences des codecs par défaut du système. Ces préférences sont affichées par les paramètres **Codec** sur un poste ou une ligne réseau IP individuelle définie sur **Configuration par défaut du système**.

En plus de modifier la préférence du codec par défaut pour tous les postes et lignes réseau VoIP, les préférences de codecs utilisés par une ligne réseau ou un poste spécifique peuvent être ajustées. Toutefois, l'utilisation des paramètres système les plus fréquemment utilisés garantit une cohérence des codecs entre les lignes réseau et les postes.

## Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez le sous-onglet **VoIP**.



La section Sélection par défaut est utilisée pour définir l'ordre des préférences des codecs par défaut. Elle est utilisée par tous les postes et lignes IP (H323 et SIP) du système dont le paramètre **Sélection du codec** est configuré sur **Configuration par défaut du système**. Il s'agit de la configuration par défaut pour tous les postes et lignes IP nouvellement ajoutés.

La liste **Codecs disponibles** indique quels sont les codecs pris en charge par le système. Les codecs de cette liste qui sont activés sont ceux pouvant être utilisés dans d'autres formes de configuration, et notamment dans la sélection par défaut adjacente.

### **Avertissement :**

Si vous désélectionnez un codec dans cette liste, il sera automatiquement supprimé des listes de codecs des lignes, systèmes ou postes où il a été utilisé.

4. Enregistrez la configuration.

## Liens connexes

[Activation du responsable de passerelle H.323](#) à la page 39

# Chapitre 5 : Paramètres DHCP

La recommandation pour l'installation des téléphones H.323 consiste à utiliser le serveur DHCP, tout particulièrement si une quantité importante de téléphones est installée. L'utilisation du serveur DHCP permet de simplifier aussi bien les interventions d'installation que de maintenance. Plusieurs options permettant de choisir le serveur qui sera utilisé pour la prise en charge DHCP des téléphones H.323 sont proposées :

- Si le système IP Office doit être utilisé comme serveur DHCP pour le réseau, suivez les procédures décrites ci-dessous pour vérifier et configurer les paramètres DHCP du système.
- Si un serveur DHCP distinct est utilisé par le réseau du client, il doit être configuré pour prendre en charge les demandes DHCP des téléphones IP.
- IP Office peut être configuré pour fournir uniquement une prise en charge DHCP pour les téléphones Avaya. Cette option peut être utilisée pour permettre une utilisation conjointe avec un serveur DHCP client distinct. Cela permet d'éliminer la nécessité de configurer le serveur DHCP du client pour la prise en charge des téléphones IP.

## Avertissement :

- L'activation d'un serveur DHCP supplémentaire sur un réseau peut entraîner des problèmes de connexion sur l'ensemble des périphériques du réseau. Assurez-vous que vous, l'utilisateur et l'administrateur réseau de l'utilisateur êtes tous d'accord sur la pertinence du choix de l'option du serveur DHCP.

## Liens connexes

[Prise en charge DHCP du système](#) à la page 43


[Numéros d'option spécifiques aux sites du système](#) à la page 44

[Modification des paramètres SSON du système](#) à la page 44

---

## Prise en charge DHCP du système

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. Sélectionnez l'onglet **Paramètres LAN**.
5. Dans **Nombre d'adresses IP DHCP**, définissez la valeur du nombre d'adresses IP que le système peut créer.

6. Sous **Mode DHCP**, sélectionnez **Serveur**.
7. Cliquez sur **Options avancées**. Les paramètres **Options avancées** permettent de configurer le paramètre **DHCP**, et notamment l'ajout de plusieurs plages de numéros **DHCP** pouvant être pris en charge par le système IP Office. Notez que les plages d'adresses situées en dehors de celles du sous-réseau des systèmes peuvent également nécessiter la création de routes IP appropriées pour garantir l'acheminement du trafic entre les sous-réseaux.

**\* Remarque :**

- Les modifications apportées aux pools DHCP ne nécessitent pas un redémarrage du système IP Office. Toutefois, cela entraîne le redémarrage des téléphones Avaya H323 et SIP connectés au système. Les téléphones IP non-Avaya ne redémarrent pas, mais devront peut-être être redémarrés manuellement afin d'obtenir une adresse valide depuis la configuration des nouveaux pools.

Cochez la case **Appliquer au téléphone IP Avaya uniquement**.

IP Office agira uniquement en tant que serveur DHCP pour les téléphones Avaya. Cette option ne peut pas être utilisée si les téléphones des séries 1100 et 1200 sont également pris en charge.

8. Enregistrez la configuration.

### Liens connexes

[Paramètres DHCP](#) à la page 43

---

## Numéros d'option spécifiques aux sites du système

Lors d'une demande de paramètres d'adresse à un serveur DHCP, chaque téléphone demande également des informations complémentaires que le serveur DHCP peut posséder en envoyant un numéro d'option spécifique au site (SSON). Si le serveur DHCP dispose d'informations correspondant au SSON, ces informations sont incluses dans la réponse DHCP.

Les téléphones des séries 1600 et 9600 utilisent le SSON 242 par défaut. Toutefois, le SSON utilisé peut être modifié dans les menus du téléphone. Pour les téléphones utilisant le système IP Office pour DHCP, les numéros SSON pris en charge par IP Office sont définis dans la configuration du système IP Office. Les valeurs utilisées par les téléphones et celles prises en charge par le système IP Office doivent concorder.

### Liens connexes

[Paramètres DHCP](#) à la page 43

---

## Modification des paramètres SSON du système

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.

2. Sélectionnez **System**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. Sélectionnez le sous-onglet **VoIP**.

The screenshot shows the configuration interface for VoIP settings. The 'DiffServ Settings' section includes fields for DSCP (Hex), Video DSCP (Hex), DSCP Mask (Hex), and SIG DSCP (Hex). The 'DHCP Settings' section is highlighted with a red box and contains fields for Primary Site Specific Option Number (4600/5600) and Secondary Site Specific Option Number (1600/9600). Other settings include VLAN, 1100 Voice VLAN Site Specific Option Number (SSON), and 1100 Voice VLAN IDs.

5. Vérifiez que les paramètres numéros d'options spécifiques au site correspondent à ceux requis par les téléphones pris en charge. Le SSON par défaut pour les téléphones des séries 1600 et 9600 est 242.
6. Enregistrez la configuration.

#### Liens connexes

[Paramètres DHCP](#) à la page 43

# Chapitre 6 : Paramètres du serveur de fichiers

Dans le cadre de la procédure d'installation, le téléphone demande les fichiers auprès d'un serveur de fichiers. À l'aide du protocole DHCP, l'adresse du serveur de fichiers est obtenue lors de la réponse DHCP provenant du serveur DHCP. L'adresse du serveur de fichiers est saisie dans le téléphone comme faisant partie intégrante de la procédure d'adressage statique.

Les options du serveur de fichiers sont les suivantes :

- Pour les systèmes IP500 V2, la carte mémoire du système IP Office peut être utilisée comme source pour les fichiers. Cette option est recommandée et peut être utilisée pour un maximum de 50 téléphones.
- Pour les systèmes IP Office Server Edition, le disque du système peut être utilisé comme source pour les fichiers utilisés par les téléphones pour la capacité totale du téléphone pris en charge par le système.
- La redirection HTTP peut être utilisée pour permettre à un serveur distant de fournir les fichiers binaires pour les téléphones 9608, 9611, 9621 et 9641 tandis que le système IP Office fournit tous les autres fichiers.
- L'application IP Office Manager peut également servir de serveur de fichiers pour un maximum de 5 téléphones. Si les options ci-dessus ne sont pas acceptables ou ne correspondent pas aux besoins de capacité du système, un serveur de fichiers HTTP tiers est requis. Les fichiers du micrologiciel requis pour les téléphones doivent être chargés sur ce serveur.

## Utilisation des ports

Le port utilisé par un téléphone IP pour demander des fichiers dépend du type de téléphone.

Port	Utilisé	Téléphones
80	Non sécurisé : micrologiciel, paramètres et données utilisateur du téléphone.	Tous
411	Sécurisé : paramètres, données utilisateur.	Téléphones 9608, 9611, 9621 et 9641 H.323
443	Sécurisé : micrologiciel, paramètres et données utilisateur du téléphone.	Téléphones SIP
8411	Non sécurisé : micrologiciel du téléphone.	Téléphones à distance H.323

Pour la plupart des nouveaux téléphones, le port à utiliser peut être indiqué via la réponse DHCP ou le fichier de paramètres du téléphone donné au téléphone. S'il n'y a pas de réponse sur ce port, le téléphone peut se replier sur l'une des valeurs de port par défaut. Cependant, certains anciens téléphones sont codés en dur aux ports fixes.

## Liens connexes

[Modification des paramètres du serveur de fichiers](#) à la page 47

[Paramètres du serveur de fichiers des téléphones](#) à la page 48

[Créer/Modifier le fichier de paramètres](#) à la page 48

[Modification manuelle du fichier](#) à la page 50

[Chargement de fichiers logiciels dans le système](#) à la page 50

[Unité de contrôle IP500 V2](#) à la page 51

[Utilisation du gestionnaire de fichiers intégré pour vérifier/charger les fichiers](#) à la page 51

[Copie manuelle des fichiers](#) à la page 52

[Chargement de fichiers sur un serveur tiers](#) à la page 53


---

# Modification des paramètres du serveur de fichiers

## À propos de cette tâche

Si le système IP Office est utilisé pour la prise en charge DHCP des téléphones IP, différents paramètres de la configuration du système IP Office sont utilisés pour définir les adresses du serveur de fichiers envoyées aux téléphones dans les réponses du serveur DHCP.

## Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Systeme**
3. Sélectionnez l'onglet **Systeme**.
4. Vérifiez le paramètre **Type de serveur de fichiers de téléphonie**. Reportez-vous à la section [Paramètres du serveur de fichiers des téléphones](#) à la page 48.
5. Dans **Type de serveur de fichiers de téléphonie**, définissez les paramètres selon vos besoins. Voir [Paramètres du serveur de fichiers des téléphones](#) à la page 48 pour plus de détails sur les différents paramètres pouvant être utilisés.
6. Pour les téléphones 9608, 9611, 9621 et 9641, sélectionnez l'option **Redirection HTTP** permettant d'envoyer des demandes de fichiers binaires de téléphone vers une autre **Adresse IP du serveur HTTP**.
7. Cochez la case **Utiliser les ports téléphoniques préférés** pour réduire l'utilisation des ports HTTP/HTTPS qui se trouvent dans la configuration de sécurité du système (par défaut, les ports 80 et 443) pour les demandes de fichiers téléphoniques.
  - Lorsque la case **Utiliser les ports téléphoniques préférés** est cochée, les fichiers de paramètres du téléphone générés automatiquement pour les téléphones régionaux indiquent le port 8411 pour HTTP et 411 pour TLS.
  - Lorsque la case **Utiliser les ports téléphoniques préférés** est décochée, les fichiers de paramètres téléphoniques générés automatiquement par le système pour les téléphones régionaux indiquent les ports 80/411 ou 80/443 en fonction du type de téléphone.

Les fichiers de paramètres du téléphone générés automatiquement par le système pour les téléphones distants indiquent les ports 8411/411 ou 8411/443 en fonction du type de téléphone.

8. Cochez la case **Clients HTTP Avaya uniquement** pour restreindre le système aux demandes de fichiers des téléphones et applications Avaya.

**\* Remarque :**

Cette option ne doit pas être utilisée si le système prend également en charge les téléphones des séries 1100 et 1200.

9. Enregistrez la configuration.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

---

## Paramètres du serveur de fichiers des téléphones

Les paramètres suivants sont utilisés pour les téléphones H323 demandant des fichiers de micrologiciel au système IP Office :

Champ	Description
<b>Carte mémoire</b> (IP500 V2) <b>Disque</b> (IP Office Server Edition)	Utilisez la mémoire du système. L'adresse IP du système est fournie en tant que valeurs du serveur de fichiers TFTP et HTTP dans la réponse DHCP. Il s'agit du paramètre par défaut.
<b>Manager</b>	Utilisez l'application IP Office Manager comme serveur de fichiers TFTP et HTTP. Cette option est uniquement prise en charge pour un maximum de 5 téléphones IP. Cette option utilise l'adresse IP du PC de Manager distincte définie dans la configuration. Le paramètre par défaut de 0.0.0.0 est utilisé par le système pour la diffusion par n'importe quelle application IP Office Manager disponible exécutée sur le réseau. Notez que par défaut, l'option IP Office Manager pour la prise en charge TFTP est désactivée ( <b>Fichier &gt; Préférences &gt; Préférences &gt; Activer les serveurs BootP et TFTP</b> ).
<b>Personnalisé</b>	Cette option utilise les valeurs distinctes de l'adresse IP du serveur TFTP et de l'adresse IP du serveur HTTP définies dans la configuration comme adresses du serveur de fichiers dans la réponse DHCP donnée aux téléphones.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

---

## Créer/Modifier le fichier de paramètres

Lors de l'installation, les téléphones demandent des fichiers en téléchargeant d'abord un fichier xxupgrade depuis le serveur de fichiers. Ils suivent ensuite les instructions contenues dans ce fichier pour demander d'autres fichiers, si nécessaire. Différents fichiers xxupgrade existent

pour chaque série de téléphones. Ils sont fournis par le firmware du téléphone. Les fichiers xxupgrade ne doivent pas être modifiés de quelque manière que ce soit.

La dernière ligne de tous les fichiers xxupgrade invite les téléphones à demander le fichier 46xxsettings.txt. Ce fichier peut être utilisé pour configurer des paramètres spécifiques au site pour l'ensemble des téléphones IP H.323 d'Avaya pris en charge sur un site particulier.

Lorsque le système IP Office est utilisé comme serveur de fichiers, le système IP Office effectue la création automatique d'un fichier 46xxsettings.txt approprié en se basant sur les différents paramètres de configuration du système IP Office. Cette opération est uniquement effectuée si aucun fichier 46xxsettings.txt physique n'est disponible sur le serveur.

### Préfixe de numérotation

Pour les systèmes IP Office, l'ajout ou la suppression des préfixes de numérotation est effectué par le système IP Office plutôt que par des téléphones individuels. L'utilisation de règles de numérotation avancées via le fichier de paramètres du téléphone n'est pas prise en charge.

### Balisage 802.1Q

À moins que des instructions contraires soient fournies expressément pour le réseau client, il est recommandé, pour un bon fonctionnement d'IP Office, de modifier la valeur ## SET L2Q 0 comme suit : SET L2Q 2.

### Langues des téléphones de série 1600/9600

En plus de l'anglais, les téléphones des séries 1600 et 9600 peuvent prendre en charge jusqu'à 4 autres langues. Pour ce faire, il faut télécharger les fichiers de langue définis dans le fichier 46xxsettings.txt. Actuellement, 9 fichiers de langues autres que l'anglais sont fournis dans le cadre de l'installation d'IP Office Manager.

Langue	Fichier 1600	Fichier 9600
Néerlandais	mlf_dutch.txt	mlf_9600_dutch.txt
Français (Canada)	mlf_french_can.txt	mlf_9600_french_can.txt
Français	mlf_french_paris.txt	mlf_9600_french_paris.txt
Allemand	mlf_german.txt	mlf_9600_german.txt
Italien	mlf_italian.txt	mlf_9600_italian.txt
Portugais	mlf_portuguese.txt	mlf_9600_portuguese.txt
Russe	mlf_russian.txt	mlf_9600_russian.txt
Espagnol	mlf_spanish.txt	mlf_9600_spanish.txt
Espagnol (Amérique latine)	mlf_spanish_latin.txt	mlf_9600_spanish_latin.txt

Les fichiers à télécharger sur les téléphones sont définis dans les sections # SETTINGS1603 # SETTINGS1608, # SETTINGS1616 du fichier 46xxsettings.txt. Pour que le téléphone télécharge un fichier de langue, supprimez les ## situés devant l'une des options SET et modifiez le nom du fichier afin qu'il corresponde à la langue voulue. Si vous utilisez le système IP Office comme serveur de fichiers, les fichiers de langue appropriés basés sur la configuration système d'IP Office peuvent être fournis en utilisant la fonction de génération automatique de fichiers.

## Sauvegarder/Restaurer

Les téléphones peuvent utiliser le serveur HTTP pour sauvegarder et restaurer les paramètres utilisateur du téléphone lorsqu'ils se connectent au téléphone ou se déconnectent. Pour plus d'informations, voir [Paramètres de sauvegarde/restauration](#) à la page 68.

## Économiseur d'écran

Vous pouvez préciser le nombre de minutes qui doivent s'écouler avant qu'un téléphone inactif affiche une image d'économiseur d'écran, de même que le nom du fichier image. Reportez-vous à la section [Économiseur d'écran](#) à la page 66.

### Liens connexes

[Paramètres du serveur de fichiers](#) à la page 46

---

## Modification manuelle du fichier

### Procédure

1. Localisez le fichier `46xxsettings.txt` sur le serveur de fichiers.
2. Ouvrez le fichier `46xxsettings.txt` à l'aide d'un outil d'édition de texte brut.
3. Modifiez le fichier selon les besoins.

Le fichier contient de nombreux commentaires et remarques. Vous trouverez des détails complémentaires sur les différents paramètres dans le manuel de l'administrateur de réseau local approprié Avaya pour le type de téléphone. Notez que les fichiers contiennent une large palette de paramètres utilisés sur d'autres systèmes téléphoniques Avaya qui ne fonctionneront pas forcément ou ne seront peut-être pas pris en charge sur les systèmes IP Office.

Un caractère # au début d'une ligne est la commande de cette ligne.

### Liens connexes

[Paramètres du serveur de fichiers](#) à la page 46

---

## Chargement de fichiers logiciels dans le système

Pour les systèmes IP Office Server Edition, le micrologiciel du téléphone adapté au fonctionnement du système IP Office est inclus dans le cadre de l'installation du système IP Office sur le serveur. Par conséquent, aucune autre action n'est nécessaire si le système est utilisé comme serveur de fichiers pour l'installation des téléphones. Le micrologiciel est également inclus dans IP Office Manager et copié sur le PC lors de l'installation d'IP Office Manager. Aucun autre micrologiciel ne doit être utilisé avec IP Office, à moins d'être expressément documenté. Le micrologiciel installé peut être vérifié et la nouvelle version peut être copiée sur le disque du système téléphonique, si nécessaire.

Le micrologiciel du téléphone adapté au fonctionnement du système IP Office est fourni avec le logiciel IP Office Manager et est copié sur le PC lorsqu'IP Office Manager est installé. Aucun autre micrologiciel ne doit être utilisé avec IP Office, à moins d'être expressément documenté.

Il existe plusieurs méthodes permettant de copier le micrologiciel installé avec IP Office sur la carte mémoire du système téléphonique. La méthode utilisée dépend principalement du type d'unité de contrôle.

 **Avertissement :**

- Il ne faut jamais retirer une carte mémoire d'un système en cours d'exécution si la carte ou le système n'a pas été désactivé au préalable. Utilisez IP Office Manager pour désactiver la carte mémoire avant de la retirer du système.
- Pour le fonctionnement d'IP Office, seuls les fichiers .bin du téléphone doivent être présents sur la carte mémoire. Les autres fichiers requis par les téléphones sont générés automatiquement par le système pour répondre aux demandes des téléphones.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

---

## Unité de contrôle IP500 V2

La carte SD du système est utilisée pour stocker les fichiers. Il s'agit d'une carte obligatoire présente dans tous les systèmes IP500 V2. Les fichiers du micro-logiciel sont chargés sur la carte de différentes manières :

- Si le système a été mis à niveau via l'option **Recréer la carte SD** disponible dans IP Office Manager, le micrologiciel est automatiquement copié sur la carte dans le cadre de cette procédure.
- Si le système a été mis à niveau à l'aide de l'assistant de mise à niveau d'IP Office Manager et si l'option **Charger les fichiers système** a été sélectionnée, alors le micrologiciel est copié sur la carte dans le cadre de cette procédure. L'option **Charger les fichiers système** est activée par défaut.

Si vous pensez que les fichiers corrects ne sont pas présents, vous pouvez utiliser le gestionnaire de fichiers intégré d'IP Office Manager pour vérifier les fichiers sur la carte et copier les fichiers sur la carte si nécessaire.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

---

## Utilisation du gestionnaire de fichiers intégré pour vérifier/charger les fichiers

### À propos de cette tâche

Le gestionnaire de fichiers intégré vous permet d'afficher à distance les fichiers se trouvant sur la carte mémoire du système téléphonique. Il permet également de charger de nouveaux fichiers.

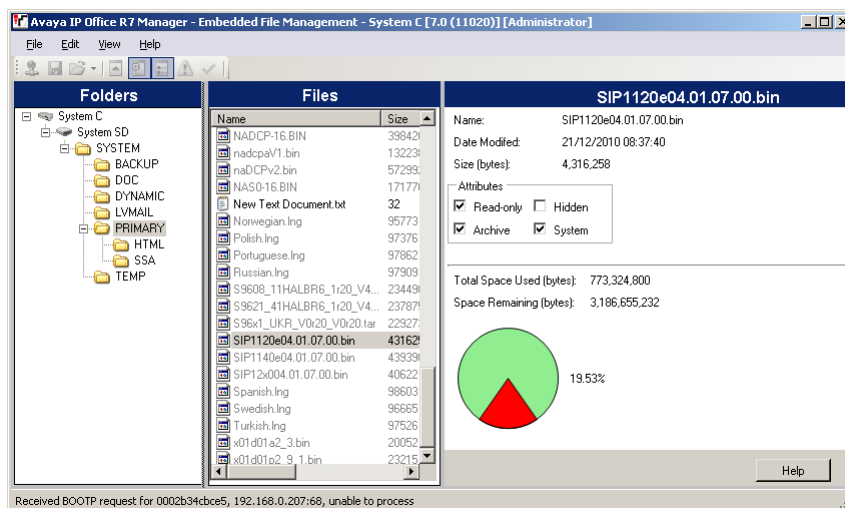
## Procédure

1. Dans IP Office Manager, sélectionnez **Fichier > Options avancées > Gestion de fichiers intégrée**.

Le menu **Sélectionner IP Office** s'affiche.

2. Sélectionnez le système téléphonique et cliquez sur **OK**.
3. Saisissez le nom et le mot de passe du système.

Le contenu de la carte mémoire est affiché.



4. Effectuez l'une des actions suivantes :
  - Pour IP500 V2, accédez à **SD Système > SYSTÈME > PRINCIPAL**.
  - Pour IP Office Server Edition, accéder à **SYSTÈME > PRINCIPAL**.
5. Pour copier les fichiers, effectuez l'une des opérations suivantes :
  - Faites glisser depuis **PRINCIPAL** vers la carte mémoire.
  - Accédez à **Fichier > Charger les fichiers système > Charger les fichiers téléphoniques** et sélectionnez le fichier à copier.

Les fichiers source se trouvent sur le PC IP Office Manager dans C:\Program Files\Avaya\IPOffice\Manager\memory Cards\Common\system\primary..

## Liens connexes

[Paramètres du serveur de fichiers](#) à la page 46

## Copie manuelle des fichiers

### À propos de cette tâche

Les fichiers peuvent être copiés sur la carte mémoire en la plaçant sur un PC équipé d'un lecteur de carte mémoire adapté.

**⚠ Avertissement :**

- Il ne faut jamais retirer une carte mémoire d'un système en cours d'exécution sans l'avoir désactivée au préalable, en suivant la procédure ci-dessous.

**Procédure**

1. Dans IP Office Manager, sélectionnez **Fichier > Options avancées > Commande de la carte mémoire > Arrêter**.

Le menu **Sélectionner IP Office** s'affiche.

2. Sélectionnez le système téléphonique et cliquez sur **OK**.
3. Saisissez le nom et le mot de passe du système.
4. Une invite vous demande quelle est la carte que vous souhaitez arrêter. Sélectionnez **Système** et cliquez sur **OK**.
5. Sur l'arrière de l'unité de commande, vérifiez que la LED du lecteur de carte mémoire est éteinte avant de retirer la carte mémoire.
6. Placez la carte dans l'emplacement pour carte mémoire du PC et visualisez le contenu.
7. Dans le système IP500 V2, accédez à **SD Système > SYSTÈME > PRINCIPAL**.

Les fichiers source se trouvent sur le PC IP Office Manager dans `C:\Program Files\Avaya\IP Office\Manager\memory Cards\Common\system\primary`.

**Résultat**

Lorsque la carte est réinsérée dans le système, l'usage de la carte est automatiquement redémarré.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

---

## Chargement de fichiers sur un serveur tiers

Les fichiers du micrologiciel du téléphone sont installés en même temps que l'application IP Office Manager et se trouvent dans le répertoire d'installation de l'application. Par défaut, le répertoire se trouve ici : `c:\Program Files\Avaya\IP Office\Manager`.

Ces mêmes fichiers de micrologiciel peuvent également être obtenus via le package logiciel utilisé pour installer IP Office Manager sans avoir à procéder à l'installation. Les fichiers se trouvent dans le sous-dossier `\program files\Avaya\IPOffice\Manager` du répertoire d'installation.

Notez que ces ensembles de fichiers comportent des fichiers `.bin` qui sont également utilisés pour d'autres périphériques, notamment le système IP Office lui-même.

**Liens connexes**

[Paramètres du serveur de fichiers](#) à la page 46

# Chapitre 7 : Création des utilisateurs et des postes

Lors de l'enregistrement d'un nouveau téléphone H.323, le système peut automatiquement ajouter un nouveau poste pour ce téléphone dans sa configuration. Il peut également créer un nouvel utilisateur pour ce téléphone. En parallèle, si le téléphone est enregistré à l'aide d'un numéro de poste pour lequel il existe déjà des entrées, ces dernières sont utilisées si aucun autre téléphone ne les utilise.

Pour de nouvelles installations, l'option Création automatique peut être utilisée pour faciliter l'ajout de plusieurs téléphones. Il est ensuite possible de désactiver les options de création automatique après l'installation. Si la fonction de création automatique n'est pas utilisée, les postes et les utilisateurs devront être ajoutés manuellement à la configuration avant toute tentative d'installation des téléphones.

## Liens connexes

[Mot de passe par défaut du poste](#) à la page 54

[Création manuelle des utilisateurs](#) à la page 55

[Création manuelle de postes](#) à la page 56

[Sélection du codec requis](#) à la page 56

[Utilisation de l'auto-création automatique](#) à la page 57

---

## Mot de passe par défaut du poste

### À propos de cette tâche

Pour l'enregistrement de la plupart des téléphones SIP, il est nécessaire de saisir un mot de passe. Cela peut être défini via le paramètre **Mot de passe par défaut du poste** du système. Vous pouvez également définir un mot de passe pour un poste spécifique dans les paramètres du poste.

Les paramètres de création automatique de poste au sein d'un système ne peuvent pas être activés tant que cette valeur n'est pas définie. Elle servira par la suite de mot de passe pour tous les postes créés automatiquement.

### Procédure

1. Chargez la configuration du système à l'aide d'IP Office Manager ou d'IP Office Web Manager en mode hors ligne.
2. Sélectionnez **Système** ou **Paramètres système** > **Système**.
3. Sélectionnez **VoIP**.

4. Sélectionnez **Sécurité VoIP**.
5. Dans la section **Mot de passe par défaut du poste** :
  - a. Cliquez sur l'icône pour afficher ou masquer le mot de passe actuel.
  - b. Si nécessaire, changez ou supprimez le mot de passe.  
Le mot de passe peut être vide ou d'une longueur comprise entre 9 et 13 chiffres (0-9).
6. Enregistrez les paramètres.

#### Liens connexes

[Création des utilisateurs et des postes](#) à la page 54


---

## Création manuelle des utilisateurs

### À propos de cette tâche

Si l'option Création automatique d'utilisateur n'est pas activée, vous devez créer manuellement un utilisateur pour chaque téléphone installé. Suivez la procédure décrite ci-dessous pour créer manuellement une entrée. Il vous est aussi demandé si vous souhaitez également créer un poste correspondant.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Pour afficher la liste des utilisateurs existants, cliquez sur  **Utilisateur**.
3. Cliquez avec le bouton droit sur le volet de droite et sélectionnez **Nouveau**.
  - a. Dans l'onglet **Utilisateur**, définissez les éléments suivants :
    - **Nom** : saisissez un nom pour l'utilisateur du poste. Ce nom doit être unique. Si l'option de messagerie vocale est activée, ce nom est repris lors de la création d'une nouvelle messagerie vocale avec un nom correspondant.
    - **Poste** : il doit correspondre au numéro de poste.
  - b. Cliquez sur **OK**.  
IP Office Manager vous invite à créer un poste correspondant.
  - c. Sélectionnez **Poste H.323** et saisissez le mot de passe du téléphone pour le poste, puis cliquez sur **OK**.
4. Enregistrez la configuration.

#### Liens connexes

[Création des utilisateurs et des postes](#) à la page 54


---

## Création manuelle de postes

### À propos de cette tâche

Si l'option Création automatique de poste n'est pas activée, vous devez créer manuellement un poste pour chaque téléphone installé. Ceci peut se faire dans le cadre de la procédure de création manuelle des utilisateurs ou séparément en suivant la procédure décrite ci-dessous.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Pour afficher la liste des postes existants, cliquez sur  **Poste**.
3. Cliquez sur **Nouveau**.
4. Dans l'onglet **Poste**, définissez les éléments suivants :
  - a. **ID du poste** : pour un poste VoIP, saisissez n'importe quel numéro unique, c'est-à-dire un numéro qui n'est utilisé par aucun autre poste.
  - b. **Poste de base** : saisissez le numéro de poste à attribuer au téléphone. Celui-ci doit également être unique. Cette valeur est utilisée pour associer le poste à l'utilisateur possédant le même numéro de poste.
  - c. **Mot de passe du téléphone** : il s'agit du mot de passe utilisé pour enregistrer le téléphone auprès du système. Si aucun mot de passe n'est défini, le **Code de connexion** de l'utilisateur correspondant est utilisé.
5. Pour ajouter le nouveau poste, cliquez sur **OK**.
6. Enregistrez la configuration.

### Liens connexes

[Création des utilisateurs et des postes](#) à la page 54

---


## Sélection du codec requis

### À propos de cette tâche

Si la **Sélection du codec** est définie sur **Configuration par défaut du système**, le poste utilise les préférences de codec du système. Cette configuration convient pour la majorité des cas. Toute modification nécessaire doit être apportée au niveau du système pour garantir la cohérence entre tous les postes et toutes les lignes réseau IP.

Toutefois, si nécessaire, la **Sélection du codec** de chaque ligne réseau et poste peut être ajustée pour être différente des paramètres par défaut du système.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Pour afficher les paramètres du poste, cliquez sur  **Poste**.
3. Sélectionnez l'onglet **VoIP**.
4. Remplacez **Sélection du codec** par **Personnalisé**.

Les listes **Non utilis\u00e9** et **S\u00e9lection** peuvent \u00eatre utilis\u00e9es pour s\u00e9lectionner les codecs que le p\u00e9riph\u00e9rique utilisera ainsi que leur ordre de pr\u00e9f\u00e9rence.

5. Enregistrez la configuration.

### Liens connexes

[Cr\u00e9ation des utilisateurs et des postes](#) \u00e0 la page 54

## Utilisation de l'auto-cr\u00e9ation automatique

### \u00c0 propos de cette t\u00e2che


Lorsque vous installez un grand nombre de t\u00e9l\u00e9phones, vous pouvez utiliser la cr\u00e9ation automatique pour simplifier le processus d'installation, sauf si la configuration a \u00e9t\u00e9 pr\u00e9construite. Les utilisateurs cr\u00e9\u00e9s de fa\u00e7on automatique sont automatiquement li\u00e9s aux param\u00e8tres de droits d'utilisateur Auto-cr\u00e9ation IP. Par d\u00e9faut, cet ensemble de droits d'utilisateur n'autorise pas les appels sortants.

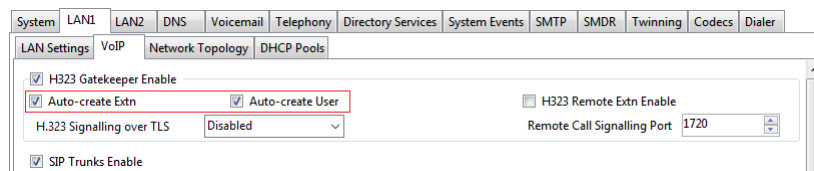
- D\u00e9sactivation automatique de la cr\u00e9ation automatique : il est vivement d\u00e9conseill\u00e9 de garder activ\u00e9s les param\u00e8tres de cr\u00e9ation automatique de postes et d'utilisateurs. Dans la version 9.1 et les versions sup\u00e9rieures, le syst\u00e8me d\u00e9sactive automatiquement les param\u00e8tres 24 heures apr\u00e8s leur activation.
- Non pris en charge avec les licences WebLM : les options de cr\u00e9ation automatique de postes et d'utilisateurs ne sont pas compatibles avec les syst\u00e8mes configur\u00e9s pour r\u00e9cup\u00e9rer des licences \u00e0 partir d'un service WebLM.

### Pr\u00e9ambules

Sur la version 11.0.4.0 et les versions ult\u00e9rieures, d\u00e9finissez le mot de passe par d\u00e9faut du poste avant d'activer la cr\u00e9ation automatique.

### Proc\u00e9dure

1. Utilisez IP Office Manager pour recevoir la configuration du syst\u00e8me.
2. S\u00e9lectionnez  **Syst\u00e8me**
3. S\u00e9lectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du syst\u00e8me que vous souhaitez utiliser pour prendre en charge les postes H.323.
4. S\u00e9lectionnez le sous-onglet **VoIP**.



5. D\u00e9finissez les param\u00e8tres **Cr\u00e9er automatiquement un poste** et **Cr\u00e9er automatiquement un utilisateur**.

### Remarque :

Il est n\u00e9cessaire de cr\u00e9er manuellement les entr\u00e9es du poste et/ou les entr\u00e9es de l'utilisateur avant de proc\u00e9der \u00e0 l'installation des t\u00e9l\u00e9phones.

Sur les versions antérieures à 11.0.4.0, lorsque l'option **Créer automatiquement un poste** est sélectionnée, définissez et confirmez un mot de passe. Le mot de passe est défini comme mot de passe du téléphone pour tous les postes créés par le biais de la création automatique. Le mot de passe du téléphone est utilisé pour l'enregistrement.

6. Enregistrez la configuration.

#### **Liens connexes**

[Création des utilisateurs et des postes](#) à la page 54

# Chapitre 8 : Connexion du téléphone


## À propos de cette tâche

Dans cette procédure, le téléphone est connecté à son alimentation ainsi qu'au réseau local Ethernet. Dès que le téléphone est mis sous tension, il commence à demander des informations.

## Préambules

Assurez-vous d'avoir terminé l'installation du téléphone avant de commencer à le connecter.

## Procédure

1. Connectez le câble LAN du réseau aux données dans la prise d'alimentation utilisée pour le téléphone.
2. Raccordez le câble LAN fourni avec le téléphone IP entre la prise de sortie d'alimentation et de données et la prise dotée d'un  de port de réseau LAN, situé à l'arrière du téléphone IP.

L'indicateur de message téléphonique doit s'illuminer en rouge pendant quelques secondes. Le téléphone démarre la procédure de chargement du logiciel. Après un bref délai, le téléphone affiche `Initialisation`, puis `Chargement`. La phase de chargement peut durer quelques minutes.

- Si le téléphone dispose déjà d'un fichier d'amorçage (c'est-à-dire, si un logiciel a déjà été installé sur ce téléphone), il charge ce fichier puis affiche `Démarrage`.
3. Si le téléphone affiche le message `Aucun Ethernet`, vérifiez que la connexion au LAN est active.

Le téléphone affiche `DHCP` ainsi qu'une minuterie pendant qu'il envoie au serveur DHCP une demande d'adresse IP, entre autres informations.

4. Appuyez sur \* lorsque `DHCP` s'affiche pour passer à l'installation de l'adresse statique. Voir installation d'adresses statiques.

La négociation DHCP prend fin après quelques secondes. Si la minuterie dépasse 60 secondes, cela indique une erreur sur le réseau ou dans la configuration du serveur DHCP.

Une fois que le serveur DHCP a terminé avec succès, le téléphone demande les fichiers provenant du serveur de fichiers indiqués dans la réponse DHCP. Le premier fichier répertorie les informations concernant les autres fichiers que le téléphone doit également charger. Le téléphone effectue sa demande de fichiers en utilisant le protocole HTTPS. En cas d'échec, il effectue la même demande en utilisant le protocole HTTP. Si cela échoue, il effectue une dernière demande en utilisant le protocole TFTP. Si toutes les requêtes de fichier échouent, le téléphone se remet à utiliser la version actuelle du fichier présent dans sa mémoire.

Le téléphone effectue un cycle de demande, de chargement et de transfert de fichiers dans la mémoire flash.

Après le chargement des fichiers, le téléphone affiche le message `Ext. =`. Reportez-vous à la section [Enregistrement du téléphone](#) à la page 60.

#### Liens connexes

[Enregistrement du téléphone](#) à la page 60

[Liste des téléphones enregistrés](#) à la page 61

---

## Enregistrement du téléphone

### À propos de cette tâche

Si un téléphone est nouveau ou qu'il a été réinitialisé, un numéro de poste doit lui être attribué.

- Si l'option de création automatique est activée, le numéro de poste utilisé, s'il est disponible, crée un nouveau poste et un nouvel utilisateur dans la configuration d'IP Office.
- Si l'option de création automatique est désactivée, le numéro de poste utilisé doit correspondre au poste VoIP enregistré dans la configuration d'IP Office. Consultez [Création manuelle de postes](#) à la page 56.

### Procédure

1. Dans **Poste**, saisissez le numéro de poste que le téléphone doit utiliser et appuyez sur #.
  - \* **Remarque :**  
Le téléphone affiche `Type modèle incorrect` si vous tentez d'utiliser le numéro d'un poste existant, étranger au réseau IP.
2. Dans **Mot de passe**, effectuez l'une des actions suivantes :
  - Si vous utilisez la création automatique pour un poste, saisissez le mot de passe spécifié lors de l'activation de la création automatique.
  - Si vous n'utilisez pas la fonction de création automatique, saisissez le **Mot de passe du téléphone** tel que défini dans la configuration du système pour le poste. Si aucun **Mot de passe du téléphone** n'a pas été défini, le système effectue une recherche en utilisant le **Code de connexion** de l'utilisateur correspondant.
  - \* **Remarque :**  
Le système désactive l'utilisation de mots de passe par défaut, tels que 0000, qui sont pris en charge par certains téléphones. Reportez-vous à la section [Blocage des codes d'accès par défaut](#) à la page 28.
3. Vérifiez que vous pouvez émettre et recevoir des appels sur le poste.

#### Liens connexes

[Connexion du téléphone](#) à la page 59

---

# Liste des téléphones enregistrés

## À propos de cette tâche

L'application System Monitor peut être utilisée pour vérifier quels sont les téléphones enregistrés dans le système.

## Procédure

1. Démarrez System Monitor et connectez-vous au système IP Office.
2. Sélectionnez **État > État du téléphone H323**.

## Résultat

System Monitor affiche les téléphones enregistrés et le nombre d'appels en attente d'enregistrement. Vous devez sélectionner l'option filtre **Système > Imprimer le suivi** pour voir ces messages.

Cela apparaît sous forme de lignes semblables à la suivante :

```
792 ms PRN : GRQ de c0a82c15 --- Le service d'accès distant atteint  
un maximum de 10 ; Points d'extrémité enregistrés 41
```

## Liens connexes

[Connexion du téléphone](#) à la page 59

# Partie 3 : Configuration facultative

# Chapitre 9 : Activation de la surveillance de la qualité du protocole RTCP

Les téléphones IP d'Avaya prennent en charge la surveillance de la qualité des appels. L'activation de la surveillance du protocole RTCP fournit au système des mesures de délai des paquets, de perte de paquets et de gigue. Vous pouvez accéder à ces informations à l'aide des applications System Status Application et System Monitor. Le système peut également être configuré pour émettre des alarmes lorsque les valeurs de qualité des appels excèdent les seuils configurés.

Il est également possible d'envoyer les rapports RTCP sur la qualité des appels à l'adresse d'une application tierce de surveillance QoS.

Pour les versions 10.0 et ultérieures d'IP Office, le système peut lui aussi envoyer des rapports RTCP concernant la qualité des appels en plus des téléphones individuels.

## Liens connexes

[Activation des rapports de qualité sur les téléphones](#) à la page 63

[Activation des rapports de qualité du système](#) à la page 64

[Configuration des seuils d'alarme de qualité](#) à la page 65


---

## Activation des rapports de qualité sur les téléphones

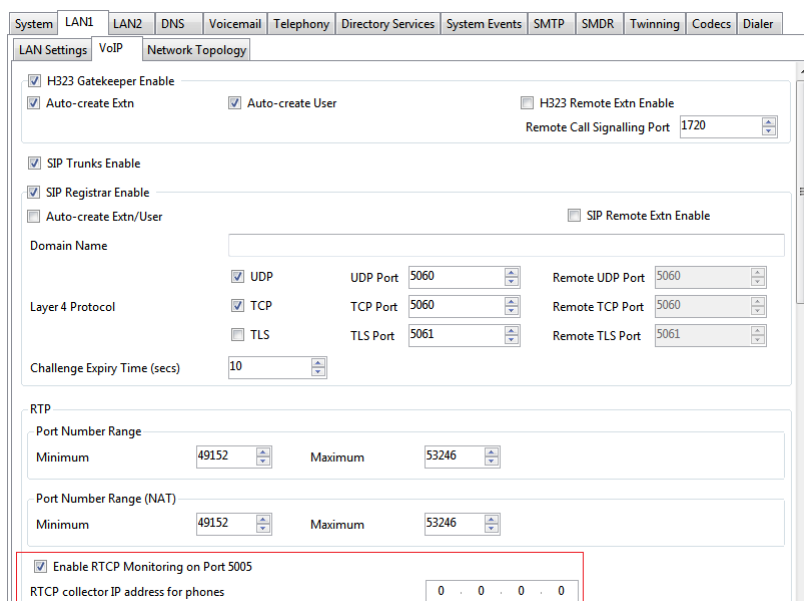
### À propos de cette tâche

L'activation des rapports de qualité des appels RTCP depuis les téléphones s'effectue centralement à partir des paramètres système.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez l'onglet **LAN1** ou **LAN2** selon les interfaces LAN du système que vous souhaitez utiliser pour prendre en charge les postes H.323.

4. Sélectionnez le sous-onglet **VoIP**.



5. Cochez la case **Activer le contrôle RTCP sur le port 5005**.

Par défaut, les données RTCP sont envoyées au système IP Office. Saisissez l'adresse dans le champ **Adresse IP du collecteur RTCP pour téléphones** pour que les données soient envoyées à une adresse spécifique par les téléphones, afin qu'elles soient collectées par une application tierce de surveillance de la QoS.

6. Enregistrez la configuration.

**Liens connexes**


[Activation de la surveillance de la qualité du protocole RTCP](#) à la page 63

## Activation des rapports de qualité du système

### À propos de cette tâche

Pour les versions 10.0 et ultérieures d'IP Office, le système peut lui aussi envoyer des rapports RTCP concernant la qualité des appels en plus des téléphones individuels.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Système**
3. Sélectionnez l'onglet **Téléphonie**, puis le sous-onglet **Téléphonie**.
4. Accédez à la section **Configuration du collecteur RTCP**.
  - a. Cochez la case **Envoyer RTCP à un collecteur RTCP**.
  - b. Dans **Adresse du serveur**, ajoutez l'adresse de l'application tierce de surveillance de la QoS à laquelle le système envoie des rapports RTCP.

- c. Dans **Numéro de port UDP**, saisissez le port de destination. La valeur par défaut est 5005.
  - d. Dans **Intervalle entre les générations de rapports RTCP**, saisissez la fréquence à laquelle le système envoie des rapports RTCP.
5. Enregistrez la configuration.

### Liens connexes

[Activation de la surveillance de la qualité du protocole RTCP](#) à la page 63


---

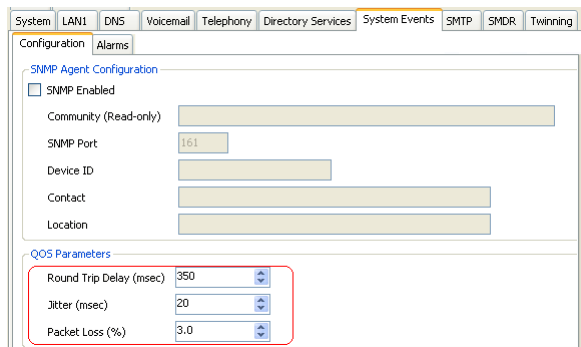
## Configuration des seuils d'alarme de qualité

### À propos de cette tâche

Le système peut envoyer des alarmes de qualité des appels à System Status Application. Il peut également envoyer ces mêmes alarmes au protocole SNMP, à des adresses électroniques ou à des destinations Syslog. Pour plus de détails sur le mode de configuration, reportez-vous à la documentation IP Office Manager. Les paramètres ci-dessous sont utilisés pour configurer les seuils qui, s'ils sont dépassés, provoquent le déclenchement d'une alarme à la fin d'un appel.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Sélectionnez  **Systeme**
3. Sélectionnez l'onglet **Événements système**, puis le sous-onglet **Configuration**.



The screenshot shows the 'System Events' configuration window in IP Office Manager. The 'Alarms' tab is active, and the 'QoS Parameters' section is highlighted with a red box. The parameters are as follows:

Parameter	Value
SNMP Enabled	<input type="checkbox"/>
Community (Read-only)	[Text Field]
SNMP Port	161
Device ID	[Text Field]
Contact	[Text Field]
Location	[Text Field]
Round Trip Delay (msec)	350
Jitter (msec)	20
Packet Loss (%)	3.0

Les paramètres QoS sont utilisés par le système pour déclencher les alarmes. Les paramètres par défaut correspondent aux seuils généralement acceptables pour une bonne qualité des appels.

4. Enregistrez la configuration.

### Liens connexes

[Activation de la surveillance de la qualité du protocole RTCP](#) à la page 63

# Chapitre 10 : Économiseur d'écran

Après un délai d'inactivité défini, les téléphones de la série 9600 peuvent afficher une image d'économiseur d'écran. Tant que le téléphone reste inactif, cette image se déplace de manière aléatoire sur l'écran toutes les 5 secondes.

Pour les téléphones pleinement pris en charge par le système IP Office, ce dernier utilise automatiquement un fichier par défaut. Si ce n'est pas le cas :

- Le délai d'inactivité activant l'économiseur d'écran et le nom du fichier image sont définis en personnalisant le fichier `46xxsettings.txt`.
- Le fichier image à utiliser doit être chargé sur le serveur de fichiers utilisé par les téléphones.

Voici les exigences en matière d'image

- Format : images JPG.
- Taille maximale des pixels : l'image doit être de plus petite taille que l'écran du téléphone. Si l'image est plus grande, elle ne s'affichera pas. Lorsque plusieurs types de téléphone utilisent la même image, la taille de cette image doit être inférieure à la taille maximale de tous les types de téléphone. Si vous utilisez le fichier `46xxsettings.txt` pour spécifier les paramètres de l'économiseur d'écran, il vous est alors possible de spécifier une image distincte pour chaque type de téléphone.

Téléphone	Taille maximale
9611	160 x 160
9621G	320 x 160
9614G	320 x 240

- Écrans couleur : profondeur de couleur de 16 bits. Une image à couleurs séparées aura un meilleur aspect.
- Affichages sans couleurs : les meilleurs résultats sont obtenus avec un seul logo en niveaux de gris. Deux niveaux sont également pris en charge.
- Transparence : pour invoquer un fond transparent, utilisez une couleur de fond 0,255,0 (vert le plus brillant possible).

Les paramètres IP Office par défaut utilisent une image nommée `96xxiposs.jpg`. À l'aide du gestionnaire de fichiers intégré dans IP Office Manager, remplacez le fichier existant dans le dossier système `/primary` par votre image personnelle. Redémarrez les téléphones afin qu'ils chargent la nouvelle image.

## Liens connexes

[Personnalisation des paramètres de l'économiseur d'écran](#) à la page 67

---

# Personnalisation des paramètres de l'économiseur d'écran

## À propos de cette tâche

Par défaut, le système utilise uniquement l'image `96xxiposs.jpg` que vous pouvez remplacer par votre propre image. Si vous utilisez un fichier `46xxsettings.txt` personnalisé, vous pouvez paramétrer le délai d'inactivité pour qu'il affiche l'économiseur d'écran et le nom de l'image.

## Procédure

1. Créez un fichier JPG client répondant aux spécifications.

Dans cet exemple, nous avons utilisé le nom de fichier `logo.jpg`.

2. Téléchargez le fichier `46xxsettings.txt` actuel à partir du serveur de fichiers utilisé par les téléphones.
3. Ajoutez les lignes suivantes au fichier `46xxsettings.txt` :

```
## SET SCREENSAVER filename
SET SCREENSAVER logo.jpg
## SET SCREENSAVER ON (délai avant l'activation, exprimé en minutes)
SET SCREENSAVERON 40
```

- Utilisation d'images distinctes pour chaque type de téléphone

Si vous ajoutez les éléments ci-dessus au début du fichier, tous les types de téléphone seront affectés. En revanche, si vous ajoutez des paramètres différents à chacune des sections MODEL4 différentes du fichier pour chaque type de téléphone, vous pourrez alors utiliser des images distinctes pour chaque type de téléphone utilisé.

4. Chargez les nouveaux fichiers sur le serveur de fichiers utilisé par les téléphones.
5. Redémarrez les téléphones afin qu'ils chargent les nouveaux paramètres et la nouvelle image.

## Liens connexes

[Économiseur d'écran](#) à la page 66

# Chapitre 11 : Paramètres de sauvegarde/ restauration

Les téléphones IP H.323 des séries 1600 et 9600 prennent en charge l'utilisation d'un serveur HTTP pour conserver les sauvegardes et restaurer les données spécifiques à l'utilisateur. L'adresse de ce serveur de sauvegarde est configurée séparément de celle du serveur de fichiers utilisé pour le firmware du téléphone.

Ces options sont utilisées si l'emplacement du serveur HTTP dédié à la sauvegarde/restauration a été défini dans le fichier `46xxsettings.txt` du téléphone.

- L'adresse du serveur HTTP utilisée pour les opérations de sauvegarde/restauration est distincte de l'adresse du serveur HTTP utilisée pour télécharger les fichiers de firmware du téléphone.
- La configuration du serveur HTTP utilisé pour la sauvegarde/restauration doit être modifiée de façon à autoriser les téléphones à envoyer des fichiers au serveur.
- Si le système IP Office est utilisé comme serveur de fichiers pour l'installation du téléphone, il peut également être utilisé pour les fonctions de sauvegarde et de restauration du téléphone. Cela inclut la génération automatique de fichiers. Lorsque vous utilisez la génération automatique, certains paramètres du fichier de restauration sont basés sur les paramètres de l'utilisateur d'IP Office. C'est, par conséquent, la solution que nous recommandons, si possible.

La sauvegarde est effectuée lorsque l'utilisateur du téléphone se déconnecte du téléphone. Au cours du processus de déconnexion, le téléphone crée un fichier contenant les données spécifiques à l'utilisateur et l'envoie à l'emplacement indiqué par l'URI de sauvegarde/ restauration (BRURI). Le nom du fichier se compose du numéro du poste de l'utilisateur utilisé comme préfixe, suivi de `_16xxdata.txt` ; par exemple, `299_16xxdata.txt`.

La restauration est effectuée lorsqu'un utilisateur se connecte au téléphone. Le téléphone envoie une demande de fichier correspondant au fichier porteur du numéro de poste de l'utilisateur. Si aucune erreur n'est rencontrée lors de la récupération du fichier, le téléphone importe les paramètres et continue de fonctionner normalement, après avoir affiché le message `Récupération réussie`. S'il est impossible de récupérer le fichier, le message `Échec de la récupération` s'affiche et le téléphone continue de fonctionner conformément aux paramètres déjà définis.

## Liens connexes

[Définition de la valeur BRURI](#) à la page 69

[Authentification HTTP](#) à la page 69

[Gestion manuelle des opérations de sauvegarde/restauration](#) à la page 70

[Exemple de fichier](#) à la page 70

---

## Définition de la valeur BRURI

### À propos de cette tâche

Si vous utilisez le système IP Office comme serveur de fichiers, nous vous recommandons de l'utiliser également comme serveur de sauvegarde et de restauration. Cette option ne nécessite aucune configuration supplémentaire. Si aucun fichier `46xxsettings.txt` n'est présent sur le système IP Office, le fichier sera créé automatiquement lorsqu'il est demandé par un téléphone et comprendra sa propre adresse IP utilisée comme adresse du serveur de sauvegarde/restauration. Si un fichier `46xxsettings.txt` est présent dans le système IP Office, vous pouvez modifier manuellement l'adresse du serveur de sauvegarde/restauration en suivant la procédure décrite ci-dessous pour la configurer afin qu'elle corresponde à l'adresse IP du système.

Si vous souhaitez utiliser un autre serveur, modifiez la valeur `BRURI` dans le fichier `46xxsettings.txt`. Vous devez également vérifier que le serveur utilisé est configuré pour autoriser le chargement des fichiers dans le dossier spécifié du serveur.

### Procédure

1. Ouvrez le fichier `46xxsettings.txt`.
2. Repérez la ligne contenant la valeur **DÉFINIR BRURI**.
3. Si la ligne est précédée de signes `#`, supprimez-les. Supprimez également tout espace en début de ligne.
4. Après `SET BRURI`, saisissez une espace, puis l'adresse du serveur de sauvegarde HTTP :
  - Par exemple, `SET BRURI http://192.168.0.28`
  - Si nécessaire, indiquez le chemin vers un répertoire de serveur spécifique et/ou mentionnez un numéro de port spécifique, par exemple : `SET BRURI http://192.168.0.28/backups:8080`.

### Liens connexes

[Paramètres de sauvegarde/restauration](#) à la page 68

---

## Authentification HTTP

L'authentification HTTP est prise en charge. Si celle-ci est activée, elle sera utilisée pour les opérations de sauvegarde et de restauration. Les informations et le domaine d'authentification sont enregistrés dans la mémoire non volatile reprogrammable du téléphone, dont les données ne sont pas écrasées lorsqu'un nouveau firmware est téléchargé sur le téléphone.

Les informations et le domaine d'authentification sont tous définis sur des valeurs nulles par défaut. Si le serveur HTTP exige des utilisateurs qu'ils s'authentifient, ceux-ci sont invités à saisir de nouvelles informations de connexion à l'aide de leur téléphone. Si l'authentification est réussie, les informations de connexion sont mémorisées et utilisées lors des opérations de sauvegarde et de restauration ultérieures.

### Liens connexes

[Paramètres de sauvegarde/restauration](#) à la page 68

## Gestion manuelle des opérations de sauvegarde/restauration

Les utilisateurs peuvent lancer une opération de sauvegarde ou de restauration à l'aide de la fonction Options **Options avancées** de sauvegarde/restauration, comme décrit dans le guide de l'utilisateur spécifique au modèle de téléphone.

### Liens connexes

[Paramètres de sauvegarde/restauration](#) à la page 68

## Exemple de fichier

Ce qui suit est un exemple de fichier de sauvegarde/restauration généré pour l'utilisateur d'un téléphone de la série 1600. Veuillez noter que ces valeurs sont enregistrées uniquement si elles ont fait l'objet d'une modification.

Si la sauvegarde et la restauration sont effectuées à l'aide de la génération automatique de fichiers, ces éléments indiqués par un \* sont contrôlés par les valeurs enregistrées et fournies par les paramètres IP Office de l'utilisateur.

Fichier	Champs	Description
ABKNAME001=Extn201 ABKNUMBER001=201 ABKNAME002=Extn201ad ABKNUMBER002=201 ABKNAME003=Extn203 ABKNUMBER003=203 Redial=0 Call Timer=0 Visual Alerting=1 Call Log Active=1 Log Bridged Calls=1 Log Line Calls=1 Log Calls Answered by Others=0 Audio Path=2 Personalized Ring=7 Handset AGC=1 Headset AGC=1 Speaker AGC=1 Error Tone=1 Button Clicks=0 Display Language=English	ABKNAMEmmm	Ces éléments vont de pair et correspondent aux contacts personnels enregistrés sur le téléphone. La valeur mmm de chaque paire est remplacée par un numéro à 3 chiffres commençant par 001. La première ligne de la paire enregistre le nom du contact et la seconde, le numéro de téléphone du contact.*
	ABKNUMBERmmm	
	LANGUSER	Langue d'affichage. Le nom de la langue est mémorisé.*
	LOGACTIVE	La journalisation des appels peut être activée (1) ou désactivée (0).*
	LOGBRIDGED	Le journalisation des appels pontés peut être activée (1) ou désactivée (0).*
	LOGLINEAPPS	La journalisation des appels de ligne peut être activée (1) ou désactivée (0).*

*Le tableau continue ...*

Fichier	Champs	Description
	LOGOTHERANS	La journalisation des appels auxquels une personne autre que le destinataire a répondu peut être activée (1) ou désactivée (0).*
	OPTAGCHAND	Le contrôle automatique de gain du combiné peut être activé (1) ou désactivé (0).
	OPTAGCHEAD	Le contrôle automatique de gain du casque peut être activé (1) ou désactivé (0).
	OPTAGCSPKR	Le contrôle automatique de gain du haut-parleur peut être activé (1) ou désactivé (0).
	OPTAUDIOPATH	Chemin audio.*
	OPTCLICKS	Les clics de boutons peuvent être activés (1) ou désactivés (0).*
	OPTERRORTONE	La tonalité d'erreur peut être activée (1) ou désactivée (0).*
	PERSONALRING	Sonnerie personnalisée. Une valeur numérique (comprise entre 1 et 8) correspondant à la sonnerie sélectionnée est mémorisée.*
	PHNRDIAL	Recomposer
	PHNSCRONCALL	L'option Écran d'appel en cas d'appel peut être activée (1) ou désactivée (0).
	PHNSCRONALERT	L'option Écran d'appel lors de la sonnerie peut être activée (1) ou désactivée (0).
	PHNTIMERS	Le chronomètre d'appel peut être activé (1) ou désactivé (0). ✓
	PHNVISUALALERT	Les alertes visuelles peuvent être activées (1) ou désactivées (0). ✓

### Liens connexes

[Paramètres de sauvegarde/restauration](#) à la page 68

[Configuration du serveur IIS](#) à la page 72

[Configuration du serveur Apache](#) à la page 72

---

## Configuration du serveur IIS

### À propos de cette tâche

Créez un dossier de sauvegarde dans le répertoire racine de votre serveur Internet. Tous les fichiers de sauvegarde seront enregistrés dans ce répertoire. Par exemple, si votre dossier de sauvegarde est `C:/Inetpub/wwwroot/backup`, le fichier `46xxsettings.txt` doit contenir la ligne suivante `SET BRURI http://www.example.com/backup`.

### Procédure

1. Dans **Démarrer > Paramètres > Panneau de contrôle > Outils d'administration**, sélectionnez, en fonction de la version Windows, **Gestionnaire des Services Internet (IIS)** ou **Services Internet (IIS)**.
2. Cliquez avec le bouton droit sur le dossier créé pour la sauvegarde. Cliquez avec le bouton droit sur **Site Internet par défaut** s'il n'existe aucun répertoire de sauvegarde spécifique.
3. Sélectionnez **Propriétés**.
4. Dans l'onglet **Répertoire**, cochez la case **Écrire**.
5. Suivez cette procédure pour configurer IIS 6.0 :
  - a. Accédez à **Démarrer > Paramètres > Panneau de contrôle > Outils d'administration**.
  - b. En dessous de **Site Internet par défaut**, sélectionnez **Poste des services Web**.
  - c. Assurez-vous que l'option **WebDAV** est définie sur **Autorisé**.

### Liens connexes

[Exemple de fichier](#) à la page 70

---

## Configuration du serveur Apache

### À propos de cette tâche

Créez un dossier de sauvegarde dans le répertoire racine de votre serveur Internet. Accordez les droits en écriture sur le dossier à tous les utilisateurs. Tous les fichiers de sauvegarde seront enregistrés dans ce répertoire. Par exemple, si le dossier de sauvegarde est `C:/Program Files/ApacheGroup/Apache2/htdocs/backup`, le fichier `46xxsettings.txt` doit contenir la ligne suivante `SET BRURI http://www.example.com/backup`.

### Préambules

#### Procédure

1. Modifiez le fichier de configuration du serveur Internet `httpd.conf`.
2. Supprimez les marques de commentaire sur les deux lignes `LoadModule` associées au protocole DAV :
  - `LoadModule dav_module modules/mod_dav.so`
  - `LoadModule dav_fs_module modules/mod_dav_fs.so`

**\* Remarque :**

Si ces modules ne sont pas disponibles sur votre ordinateur, ce qui est généralement le cas sur certains serveurs Apache Unix/Linux, vous devez effectuer une nouvelle fois la compilation de ces deux modules (mod\_dav et mod\_dav\_fs) afin de les intégrer au serveur. Il se peut que vous disposiez d'autres méthodes de chargement de ces modules. Pour en savoir plus, consultez votre documentation Apache à l'adresse suivante : <http://httpd.apache.org/docs/>.

3. Ajoutez les lignes suivantes au fichier `httpd.conf` :

```
#
#WebDAV configuration
#D
avLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
<Location />
Dav On
</Location>
```

**\* Remarque :**

Pour les serveurs Web Unix/Linux, la quatrième ligne peut être formulée comme suit : `DavLockDB/usr/local/apache2/var/DAVLock`

4. Créez un répertoire `var` et accordez les droits en écriture sur ce répertoire à tous les utilisateurs. Cliquez avec le bouton droit sur **Propriétés** et sélectionnez **Sécurité > Ajouter > Tout le monde > Contrôle total > .**

**Liens connexes**

[Exemple de fichier](#) à la page 70

# Partie 4 : Processus d'installation avancés

# Chapitre 12 : Installation d'adresses statiques

Les adresses statiques ne sont nécessaires que lorsqu'aucun serveur DHCP n'est disponible ou utilisé. Afin de faciliter la maintenance et l'installation, assurez-vous qu'un serveur DHCP est utilisé et évitez les adresses statiques. Suivant la mise à niveau du fichier d'amorçage du micrologiciel du téléphone, les informations relatives aux adresses statiques peuvent nécessiter une réinstallation.

## Liens connexes

[Installation de l'adresse statique pour les téléphones de la série 1600](#) à la page 75

[Paramètres d'installation de l'adresse statique pour les téléphones de la série 1600](#) à la page 76

[Installation de l'adresse statique pour les téléphones de la série 9600](#) à la page 77

[Paramètres d'installation de l'adresse statique pour les téléphones de la série 9600](#) à la page 77

---

## Installation de l'adresse statique pour les téléphones de la série 1600

### Procédure

1. Terminez la procédure de connexion du téléphone et, lorsque DHCP s'affiche, appuyez sur \* pour basculer le téléphone sur l'installation d'adresse statique.

Le téléphone affiche alors tour à tour des paramètres et les valeurs définies pour chacun de ces paramètres.

2. Appuyez sur la touche # pour accepter les valeurs actuelles ou saisissez une valeur et appuyez sur la touche #. Reportez-vous à la section [Paramètres d'installation de l'adresse statique pour les téléphones de la série 1600](#) à la page 76.

**\* Remarque :**

Si aucune valeur n'est modifiée, le téléphone affiche `No new values` (Aucune nouvelle valeur).

3. Si le téléphone affiche le message `Enter` (Entrer), éteignez le téléphone et rallumez-le.

Une fois que toutes les valeurs ont été saisies ou que les valeurs existantes ont été acceptées, le téléphone affiche le message suivant : `Save new values?` (Enregistrer les nouvelles valeurs ?).

4. Appuyez sur # pour enregistrer les valeurs.

### Étapes suivantes

Enregistrez le téléphone.

### Liens connexes

[Installation d'adresses statiques](#) à la page 75

---

## Paramètres d'installation de l'adresse statique pour les téléphones de la série 1600

Nom des paramètres	Description
<b>Téléphone</b>	Il s'agit de l'adresse IP du téléphone. Appuyez sur la touche # pour accepter la valeur actuelle ou saisissez une valeur et appuyez sur la touche #. Si vous saisissez une nouvelle valeur, appuyez sur la touche * pour saisir un point (.) entre des chiffres.
<b>CallSv</b>	Il s'agit de l'adresse du responsable de passerelle H.323. Pour les systèmes IP Office, il s'agit de l'adresse IP du LAN IP Office.
<b>CallSvPort</b>	Il s'agit du numéro de port de la couche d'acheminement du responsable de passerelle. Pour les téléphones IP Avaya, ce paramètre doit être défini sur 1719. Appuyez sur la touche # pour accepter la valeur actuelle ou saisissez une valeur et appuyez sur la touche #.
<b>Routeur</b>	Il s'agit de l'adresse de la passerelle IP par défaut du téléphone. Pour IP Office, il s'agit généralement de l'adresse IP du réseau local LAN IP Office. Appuyez sur la touche # pour accepter la valeur actuelle ou saisissez une valeur et appuyez sur la touche #.
<b>Masquer</b>	Il s'agit du masque IP du téléphone (également appelé masque de sous-réseau). Ce masque permet à l'adresse IP d'indiquer le sous-réseau auquel le téléphone appartient. Il doit correspondre au masque IP défini pour l'unité IP Office.
<b>FileSv</b>	Il s'agit de l'adresse du serveur de fichiers auquel le téléphone doit envoyer toute demande de fichier logiciel ou de paramètres. Saisissez l'adresse du serveur TFTP ou HTTP configuré sur l'ensemble des fichiers logiciels du téléphone IP Avaya.
<b>802.1Q</b>	Pour modifier ce paramètre, appuyez sur la touche *. Appuyez sur la touche # pour accepter cette valeur.
<b>ID de VLAN</b>	Pour plus d'informations sur la configuration du VLAN, consultez VLAN et téléphones IP.

### Liens connexes

[Installation d'adresses statiques](#) à la page 75

## Installation de l'adresse statique pour les téléphones de la série 9600

### Procédure

1. Lorsque `* to program` (\* à programmer) s'affiche, appuyez sur la touche `*`.
2. Lorsque l'option `Entrer le code` s'affiche, saisissez le mot de passe des procédures administratives, puis appuyez sur `#`. Le mot de passe par défaut est CRAFT (27238).
3. Faites défiler le menu pour accéder à ADDR, puis sélectionnez cette option pour démarrer la procédure d'adresse.

La liste des adresses requises s'affiche. Si des valeurs de téléphone existantes s'affichent. Sinon, si le téléphone est neuf ou a été effacé, toutes les adresses sont configurées sur 0.0.0.0.

4. Pour chaque adresse, mettez en surbrillance la valeur à modifier et cliquez sur **Modifier**. Reportez-vous aux paramètres d'installation de l'adresse statique.
5. Saisissez la nouvelle adresse, puis sélectionnez **Enregistrer**.
6. Une fois toutes les valeurs définies comme requises, cliquez sur **Retour**, puis sur **Quitter**.

Le téléphone redémarre en utilisant les nouvelles valeurs.

### Étapes suivantes

Enregistrez le téléphone.

### Liens connexes

[Installation d'adresses statiques](#) à la page 75

## Paramètres d'installation de l'adresse statique pour les téléphones de la série 9600

Nom des paramètres	Description
<b>Téléphone</b>	Il s'agit de l'adresse IP du téléphone. Appuyez sur la touche <code>#</code> pour accepter la valeur actuelle ou saisissez une valeur et appuyez sur la touche <code>#</code> . Si vous saisissez une nouvelle valeur, appuyez sur la touche <code>*</code> pour saisir un point ( <code>.</code> ) entre des chiffres.
<b>Serveur d'appels</b>	Il s'agit de l'adresse du responsable de passerelle H.323. Pour les systèmes IP Office, il s'agit de l'adresse IP du LAN IP Office.
<b>Routeur</b>	Il s'agit de l'adresse de la passerelle IP par défaut du téléphone. Pour IP Office, il s'agit généralement de l'adresse IP du réseau local LAN IP Office. Appuyez sur la touche <code>#</code> pour accepter la valeur actuelle ou saisissez une valeur et appuyez sur la touche <code>#</code> .

*Le tableau continue ...*

Nom des paramètres	Description
<b>Masquer</b>	Il s'agit du masque IP du téléphone (également appelé masque de sous-réseau). Ce masque permet à l'adresse IP d'indiquer le sous-réseau auquel le téléphone appartient. Il doit correspondre au masque IP défini pour l'unité IP Office.
<b>Serveur de fichiers HTTP</b>	Il s'agit de l'adresse du serveur de fichiers HTTP auquel le téléphone doit envoyer toute demande de fichier logiciel ou de paramètres.
<b>Serveur de fichiers HTTPS</b>	Il s'agit de l'adresse du serveur de fichiers HTTPS auquel le téléphone doit envoyer toute demande de fichier logiciel ou de paramètres. Le téléphone tente d'utiliser cette adresse, si elle a été définie, avant d'utiliser le protocole HTTP.
<b>802.1Q</b>	Pour modifier ce paramètre, appuyez sur la touche *. Appuyez sur la touche # pour accepter cette valeur.
<b>ID de VLAN</b>	Pour plus d'informations sur la configuration du VLAN, consultez VLAN et téléphones IP.
<b>Test VLAN</b>	Lors de l'utilisation d'un VLAN, il s'agit de la durée en secondes pendant laquelle le téléphone attendra une réponse de la part du serveur DHCP dans le VLAN avant de revenir à un fonctionnement normal (différent du VLAN).

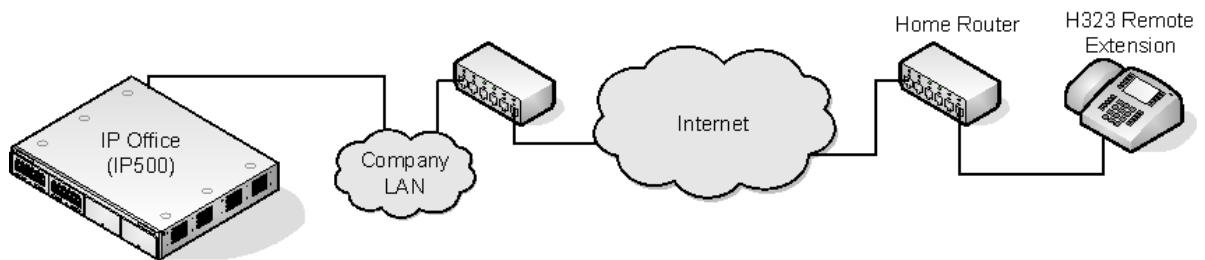
### Liens connexes

[Installation d'adresses statiques](#) à la page 75

# Chapitre 13 : Postes H.323 distants

Pour les versions 8.0 et ultérieures d'IP Office, la configuration des postes distants H.323 est prise en charge sans que ces postes n'aient à fonctionner sous un micrologiciel VPN spécial. Cette option est destinée à être utilisée dans le scénario suivant :

- Le LAN du client dispose d'une adresse IP publique qui est renvoyée au système IP Office. Cette adresse est utilisée comme adresse pour le serveur d'appels par les postes distants H.323.
- L'utilisateur dispose d'un téléphone H.323 derrière un routeur national. Nous partons du principe que le routeur national autorise le passage de tout le trafic entrant provenant du réseau domestique ainsi que tout le trafic symétrique. En effet, si le téléphone envoie le protocole RTP/RTCP vers une adresse IP et un port publics, il peut recevoir le protocole RTP/RTCP en provenance de cette même adresse IP et de ce même port. Les autres types de configurations ne sont pas abordés dans cette documentation.



- Le système peut être configuré pour la prise en charge des postes distants H.323 lorsque le mode NAT est utilisé dans le chemin de connexion. C'est le cas, par exemple, lorsqu'IP Office est situé derrière un routeur NAT/pare-feu d'entreprise et/ou lorsque le téléphone H.323 se trouve derrière un routeur NAT résidentiel. L'utilisation de cette option, ainsi que l'interaction et la configuration d'éléments tiers externes, ne sont pas traités dans ce fichier d'aide.
- Lorsque l'adresse IP publique du routeur d'entreprise n'est pas connue, vous devez configurer un serveur STUN dans les paramètres Topologie réseau LAN d'IP Office. Veuillez toutefois noter que cette option n'est pas prise en charge si le Type de pare-feu/NAT est défini sur Pare-feu symétrique ou sur Connexion directe à Internet.
- L'activation de l'option Autoriser le poste distant rend également visible la configuration des paramètres Plage de numéros de ports RTP (NAT).
- Téléphones pris en charge : actuellement, le fonctionnement des postes H.323 distants est uniquement pris en charge par les téléphones de la série 9600 déjà pris en charge par le système IP Office.
- Conditions de licence : par défaut, seuls 4 utilisateurs peuvent être configurés pour l'utilisation du poste distant H.323 sans licence. D'autres utilisateurs peuvent être configurés s'ils bénéficient d'une licence et s'ils ont été configurés avec un profil utilisateur **Teleworker** ou **Power User**.

**Liens connexes**

[Configuration du réseau client](#) à la page 80

[Configuration du système IP Office \\*](#) à la page 81

[Configuration des téléphones](#) à la page 82

---

## Configuration du réseau client

Le LAN d'entreprise hébergeant le système IP Office requiert une adresse IP publique acheminée vers l'interface LAN du système IP Office configurée pour la prise en charge des postes distants H.323.

Le serveur STUN partant du système IP Office vers Internet est utilisé pour déterminer le type de NAT appliqué au trafic entre le système et Internet. Les routeurs et autres pare-feu situés entre l'emplacement des téléphones H.323 et le système IP Office doivent autoriser le trafic suivant.

Protocole	Port	Description
ICMP	-	L'ICMP entrant de l'adresse IP publique du système IP Office doit être autorisé.
UDP	1719	Le trafic UDP du port 1719 vers le système IP Office doit être autorisé. Il est utilisé pour les processus H225 RAS, tels que la reconnaissance des responsables de passerelle, l'enregistrement, la conservation des connexions actives, etc. Si ce port n'est pas ouvert, le téléphone ne peut s'enregistrer dans le système IP Office.
TCP	1720	Le trafic TCP entrant sur le port 1720 doit être autorisé. Il est utilisé pour H.225 (signalisation d'appel). Il est possible de modifier l'adresse utilisée à l'aide du paramètre Port de signalisation d'appel distant.
RTP	Divers	Les ports compris dans la plage spécifiée par les paramètres Plage de numéros de port RTP (NAT) du système doivent être autorisés.
RTCP		
UDP	5005	Si le paramètre système Activer le contrôle RTCP sur le port 5005 a été activé, le trafic sur ce port doit être autorisé pour le contrôle inclue les postes H.323 distants.

### Configuration réseau par l'utilisateur

Nous partons du principe que le routeur national autorise le passage de tout le trafic entrant provenant du réseau domestique ainsi que tout le trafic symétrique. Ainsi, si le téléphone envoie un RTP/RTCP à une adresse IP publique et un port, le routeur l'autorisera à recevoir un RTP/RTCP de ces mêmes adresse IP et port.

**Liens connexes**

[Postes H.323 distants](#) à la page 79

# Configuration du système IP Office \*

## À propos de cette tâche

Il s'agit d'un résumé des modifications nécessaires dans la configuration du système IP Office. Cette section part du principe que vous vous êtes familiarisé avec le système IP Office et l'installation du téléphone IP H.323.

## Préambules

Si plus de 4 utilisateurs de postes distants doivent être pris en charge, le système doit comprendre des licences **Teleworker** et/ou **Power User** pour ces utilisateurs.

## Procédure

1. Dans l'onglet **Système**, configurez les éléments suivants :

- a. Accédez à **Système** > **LAN1** > **LAN2** > **VoIP**.
- b. Cochez la case **Activer le responsable de passerelle H.323**.

 **Remarque :**

En raison des paramètres utilisateur et de poste supplémentaires requis pour la configuration des postes H.323 distants, les postes et les utilisateurs des postes H.323 distants et les utilisateurs sont ajoutés manuellement.

- c. Activez **Activer les postes distants H.323**.
- d. Saisissez la valeur requise dans **Port de signalisation d'appel distant**.

La valeur par défaut de 1720 correspond également au port utilisé par les postes internes.

- e. Configurez le paramètre **Plage de numéros de ports RTP (NAT)** pour qu'il englobe la plage de ports devant être utilisée pour le trafic RTP et RTCP des postes H.323 distants.

 **Remarque :**

La configuration de cette plage doit fournir au minimum deux ports par poste pris en charge.

2. Dans l'onglet **Topologie réseau**, configurez les éléments suivants :

 **Remarque :**

Le serveur STUN peut être utilisé pour déterminer le type de processus NAT/pare-feu appliqué au trafic entre le système IP Office et Internet.

- a. Accédez à **Topologie réseau** et configurez le champ **Adresse IP du serveur STUN** sur un serveur STUN connu.
- b. Cliquez sur **OK**.

Le bouton **Exécuter STUN** est activé.

- c. Cliquez sur **Exécuter STUN**, puis patientez jusqu'à ce que le processus STUN s'exécute.

Les résultats révélés par ce processus sont affichés par les icônes ! situées à côté des champs.

- d. Si STUN signale le **Type de pare-feu/NAT**, le réseau doit être reconfiguré.

**\* Remarque :**

Les types de réseaux **Bloc de ports statiques**, **NAT symétrique** ou **Connexion directe à Internet** ne sont pas pris en charge pour les postes H.323 distants.

3. Dans l'onglet **Utilisateur**, configurez les éléments suivants :
  - a. Accédez à l'onglet **Utilisateur** et définissez le **Profil de l'utilisateur** sur **Teleworker** ou **Power User**.
  - b. Activez **Autoriser Travailleur distant**.

**Liens connexes**

[Postes H.323 distants](#) à la page 79

---

## Configuration des téléphones

Les téléphones ne requièrent pas l'utilisation d'un micrologiciel spécial. Par conséquent, ils doivent d'abord être installés comme des postes internes normaux. Ensuite, ils chargeront le micrologiciel fourni par le système IP Office.

Une fois cette procédure terminée, les paramètres d'adresse du téléphone doivent être effacés et l'adresse du serveur d'appels, configurée sur l'adresse publique à utiliser par les postes H.323 distants.

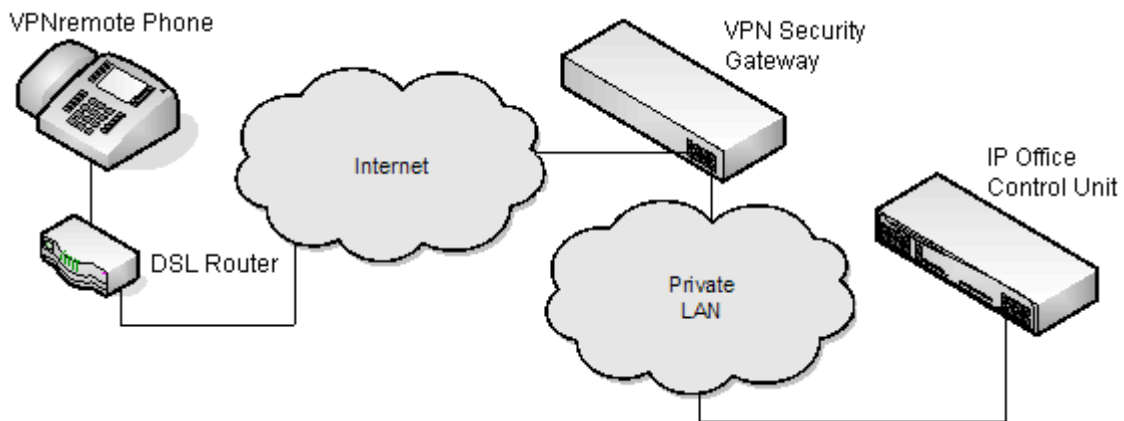
Nous partons du principe qu'à l'emplacement distant, le téléphone obtiendra d'autres informations d'adresse par le DHCP du routeur de l'utilisateur. Dans le cas contraire, l'autre paramètre d'adresse du téléphone doit être administré statiquement pour correspondre aux adresses adaptées pour le réseau domestique de l'utilisateur.

**Liens connexes**

[Postes H.323 distants](#) à la page 79

# Chapitre 14 : Téléphones VPN distants

Les téléphones IP Avaya installés sur des sites distants peuvent être connectés au système IP Office via des tunnels VPN IPSec. Cette option est prise en charge sur les téléphones des séries 4610SW, 4621SW, 5610SW et 5621SW. Elle est également prise en charge sur les téléphones de la série 9600.



Les composants supplémentaires requis pour les téléphones distants via VPN sont les suivants :

- Micrologiciel du téléphone VPN distant IP Office : ce micrologiciel est inclus dans l'ensemble de micrologiciels du téléphone IP.
- Passerelle de sécurité VPN : le système IP Office ne prend pas en charge toutes les fonctionnalités IPSec requises par les téléphones VPN distants utilisant leurs propres tunnels IPSec. Par conséquent, le tunnel VPN des téléphones distants doit se terminer au niveau d'un autre périphérique de passerelle VPN adapté. Ce périphérique doit prendre en charge l'une des méthodes suivantes :
  - Passerelles Avaya : les périphériques de passerelles de sécurité Avaya, (SG ou VSU) utilisent un protocole propre à Avaya appelé
    - CCD des passerelles de sécurité Avaya SG Series (micrologiciel version 4.6 ou ultérieure)
    - Unités de services VPN Avaya VSU Series (micrologiciel version 3.2 ou ultérieure)
  - Passerelles non-Avaya : passerelles VPN non-Avaya dotées de l'authentification étendue IKE (Xauth) avec clé pré-partagée (PSK). Des notes concernant leur installation sont disponibles pour les passerelles répertoriées ci-dessous. Ceci n'implique pas la recommandation de ces périphériques par Avaya ni n'exclut d'autres périphériques.

**\* Remarque :**

Avaya ne peut pas garantir la prise en charge des services fournis par l'intermédiaire de périphériques de marques autres qu'Avaya.

- Concentrateurs VPN Cisco 300 Series
- Pare-feu Cisco PIC 500 Series
- Périphériques VPN Juniper Networks NetScreen Series
- Plate-forme de sécurité Secure Services Gateway 500 Series de Juniper Networks
- Passerelle de sécurité intégrée (ISG) Series Juniper Networks
- Routeur VPN Kentrox Q2300
- Routeur VPN Sonicwall Tz170
- Routeur VPN Netgear FVS338
- Routeur VPN Netgear FVX538
- Routeur VPN Adtran Netvanta 3305

**Liens connexes**

[Documentation d'installation](#) à la page 84

[Micrologiciel du téléphone VPN distant pris en charge](#) à la page 84

[Configuration du VPN distant sur un téléphone IP](#) à la page 85

[VLAN et téléphones IP](#) à la page 85

[VLAN et DHCP](#) à la page 86

[Exemple de configuration : présentation](#) à la page 87

[Présentation d'un exemple de système](#) à la page 90

---

## Documentation d'installation

Le présent document fait uniquement état de remarques et de particularités spécifiques à l'installation de téléphones VPN distants avec IP Office. Ensuite, l'installation et la configuration des téléphones VPN distants d'Avaya sont décrites dans plusieurs autres documents disponibles sur le site d'assistance d'Avaya (<http://support.avaya.com>). Reportez-vous au *Guide de configuration du VPN pour les téléphones IP de la série 9600*, référence du document : 16-602968.

**Liens connexes**

[Téléphones VPN distants](#) à la page 83

---

## Micrologiciel du téléphone VPN distant pris en charge

Sauf indication contraire, seul le micrologiciel disponible sur le DVD des applications administrateur d'IP Office doit être utilisé pour les téléphones VPN distant reliés à un système IP Office. Ce micrologiciel est testé avec la version d'IP Office pour un fonctionnement correct. Le micrologiciel se trouve dans un fichier zip du dossier `\bin\VPN Phone`.

Il est possible qu'Avaya ait mis à votre disposition d'autres versions de ce micrologiciel pour VPN distant à télécharger. Toutefois, ces versions peuvent ne pas avoir été testées avec IP Office.

#### Liens connexes

[Téléphones VPN distants](#) à la page 83


---

## Configuration du VPN distant sur un téléphone IP

### À propos de cette tâche

En outre, la case à cocher Téléphone VPN autorisé s'affiche dans l'onglet des paramètres **Poste > VoIP** des postes IP. La case **VoIP** permet de signaler au système IP Office les postes de type VPNremote, qui doivent disposer d'une licence.

### Procédure

1. Utilisez IP Office Manager pour recevoir la configuration du système.
2. Cliquez sur  **Poste**, puis sélectionnez l'entrée correspondant au poste IP concerné.
3. Sélectionnez l'onglet **VoIP**.
4. Activez **Téléphone VPN autorisé**.
5. Cliquez sur **OK**.
6. Renouvelez cette démarche pour tous les autres postes IP qui vont être dotés d'une connexion VPN.
7. Enregistrez la configuration.

#### Liens connexes

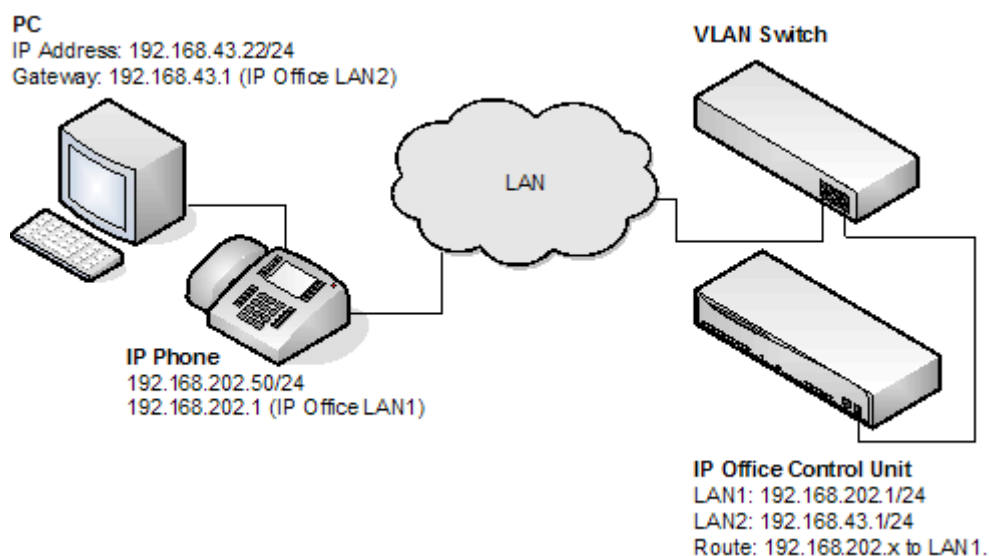
[Téléphones VPN distants](#) à la page 83

---

## VLAN et téléphones IP

L'utilisation du VLAN permet de créer des domaines de collision distincts sur les commutateurs Ethernet. En ce qui concerne IP Office et les téléphones IP, les avantages sont les suivants :

- Il permet aux ordinateurs de demeurer dans le même sous-réseau IP, tandis que les téléphones IP peuvent utiliser un nouveau schéma d'adressage IP distinct.
- Le réseau de données de l'ordinateur ne diffuse aucun trafic sur le réseau vocal des téléphones IP, et inversement. Ceci garantit de meilleures performances, car dans le cas contraire, le trafic diffusé doit être évalué par tous les destinataires.
- Les réseaux VLAN et la classification du trafic par ordre de priorité sur la couche 2 sont étroitement liés par la norme 802.2. Il est donc plus facile d'assurer la qualité de service de la couche 2 (L2 QoS) lorsque vous utilisez un VLAN.



Le tableau indique les trois manières de déployer un VLAN doté d'un commutateur Ethernet. Étant donné que les deux premières méthodes sont très simples et que le présent document suppose que l'ordinateur et les téléphones IP sont dotés du même port Ethernet, celui-ci décrira la troisième méthode (chevauchement) plus en détail.

Type	Description	Avantages	Inconvénients
Aucun VLAN	Les réseaux vocaux et de données se trouvent sur le même domaine de collision	Configuration simple	Le trafic diffusé par l'ordinateur entrave le trafic vocal. Nécessite deux (2) ports par utilisateur (un pour le téléphone IP et un autre pour l'ordinateur)
VLAN physique	Réseaux VLAN distincts pour les données et les signaux vocaux	Configuration simple	Nécessite deux (2) ports par utilisateur (un pour le téléphone IP et un autre pour l'ordinateur)
VLAN se chevauchant	Un seul port du commutateur prend en charge à la fois le trafic du téléphone IP et celui de l'ordinateur	Nécessite un seul port pour l'ordinateur et le téléphone IP  Le trafic diffusé par l'ordinateur n'entraîne aucune gêne du trafic vocal	Configuration complexe

### Liens connexes

[Téléphones VPN distants](#) à la page 83

## VLAN et DHCP

L'utilisation d'un VLAN a des conséquences sur le DHCP si celui-ci est utilisé pour la prise en charge des téléphones IP ou des ordinateurs. Le tableau ci-dessous répertorie les options

disponibles lorsque les téléphones IP et les ordinateurs d'un réseau sur lequel VLAN est activé sont pris en charge par un seul et même port.

Option DHCP	Description
Aucun (adressage statique)	Configuration manuelle de chaque téléphone IP
Serveurs DHCP distincts	Deux PC, un pour chaque VLAN
Serveur DHCP multihébergé	Un seul PC doté de deux cartes NIC, une pour chaque VLAN
Relais DHCP	Cette option doit être prise en charge par le commutateur Ethernet

S'il utilise le DHCP, le téléphone IP, au moment du démarrage, cherche d'abord à détecter une requête DHCP sans balise VLAN.

- Si la réponse DHCP contient un nouveau paramètre VLAN dans le champ d'application SSON, les téléphones délivrent toutes ses adresses IP et effectuent une nouvelle requête DHCP en utilisant l'ID du VLAN nouvellement fourni.

Si le téléphone IP ne reçoit pas de nouvel ID VLAN, il continue de fonctionner avec les paramètres fournis dans la réponse DHCP d'origine.

Un ID VLAN peut également être transmis à un téléphone via le fichier qu'il charge. Le téléphone IP délivre à nouveau tous ses paramètres IP existants, puis effectue une nouvelle requête DHCP en utilisant l'ID VLAN nouvellement fourni.

Dans l'exemple ci-dessous, lorsque les téléphones IP reçoivent une réponse DHCP de la part du serveur DHCP sur le VLAN de données, cette réponse contient l'ID du VLAN vocal. Le téléphone délivre ensuite les paramètres du VLAN de données d'origine qu'il a obtenus et envoie une nouvelle requête DHCP au VLAN vocal.

Option	Paramètres DHCP du VLAN de données	Paramètres DHCP du VLAN vocal
Adresse IP	192.168.43.x	192.168.202.x
Masquer	255.255.255.0	255.255.255.0
Routeur	192.168.43.1	192.168.202.1
SSON Champ d'application	L2Q=1, L2QVLAN=202, VLANTEST=0	MCIPADD=192.168.202.1, MCPORT=1719, HTTPSRVR=192.168.202.X VLANTEST=0
Le paramètre VLANTEST correspond à la durée pendant laquelle un téléphone IP doit continuer d'envoyer des demandes au serveur DHCP au sein d'un VLAN (0 indique une durée illimitée).		

### Liens connexes

[Téléphones VPN distants](#) à la page 83

## Exemple de configuration : présentation

Le réseau est conçu pour permettre au PC de l'utilisateur de se connecter au port de commutation du téléphone IP. Un seul câble relie alors le PC et le téléphone IP au

commutateur Ethernet. Dans le présent exemple, le VLAN 100 est dédié au trafic vocal et le VLAN 101 au trafic de données. L'interface du LAN1 de l'unité de contrôle d'IP Office se trouve sur le VLAN vocal, tandis que l'interface du LAN2 se trouve sur le VLAN de données. La communication entre les VLAN vocal et de données s'effectue grâce à la fonction de routeur remplie par l'unité de contrôle d'IP Office.

## Configuration du commutateur HP

Vous trouverez ci-dessous les données de configuration Web et CLI du commutateur HP Procurve. Pour effectuer ce type de configuration, suivez les instructions ci-dessous.

The screenshot shows the HP Procurve web configuration interface. The top navigation bar includes tabs for Identity, Status, Configuration (selected), Security, Diagnostics, and Support. Below the navigation bar, there are several sub-tabs: Device View, Fault Detection, System Info, IP Configuration, Port Configuration, Monitor Port, Device Features, Stacking, VLAN Configuration (selected), and Support/Mgmt URL. The main content area displays a table of VLAN configurations:

VLAN ID	VLAN Name	VLAN Type	Tagged Por	Untagged Ports	Forbid Ports	Auto	
1	Native (Prim	STATIC	(STATIC) None (GVRP) None	1-2,4, 7-26	None	3,5-6	Modify
100	Red [Voice]	STATIC	(STATIC) 3 (GVRP) None	5	None	1-2,4, 6-26	Modify
101	Blue [Data]	STATIC	(STATIC) None (GVRP) None	3,6	None	1-2,4-5, 7-26	Modify

At the bottom of the interface, there are buttons for "ADD/REMOVE VLANs", a checkbox for "GVRP Enabled" (checked), and a "GVRP Mode" button.

### HP Procurve CLI output

```
; J8164A Configuration Editor; Created on release #H.08.60

hostname "AvayaLabs"
snmp-server community "public" Unrestricted
vlan 1
name "Native"
untagged 1-2,4,7-26
ip address 192.168.202.201 255.255.255.0
no untagged 3,5-6
exit
vlan 100
name "Red [Voice]"
untagged 5
tagged 3
exit
vlan 101
name "Blue [Data]"
untagged 3,6
exit
gvrp
spanning-tree
```

Le tableau ci-dessous récapitule la configuration des ports et des VLAN pour le commutateur HP.

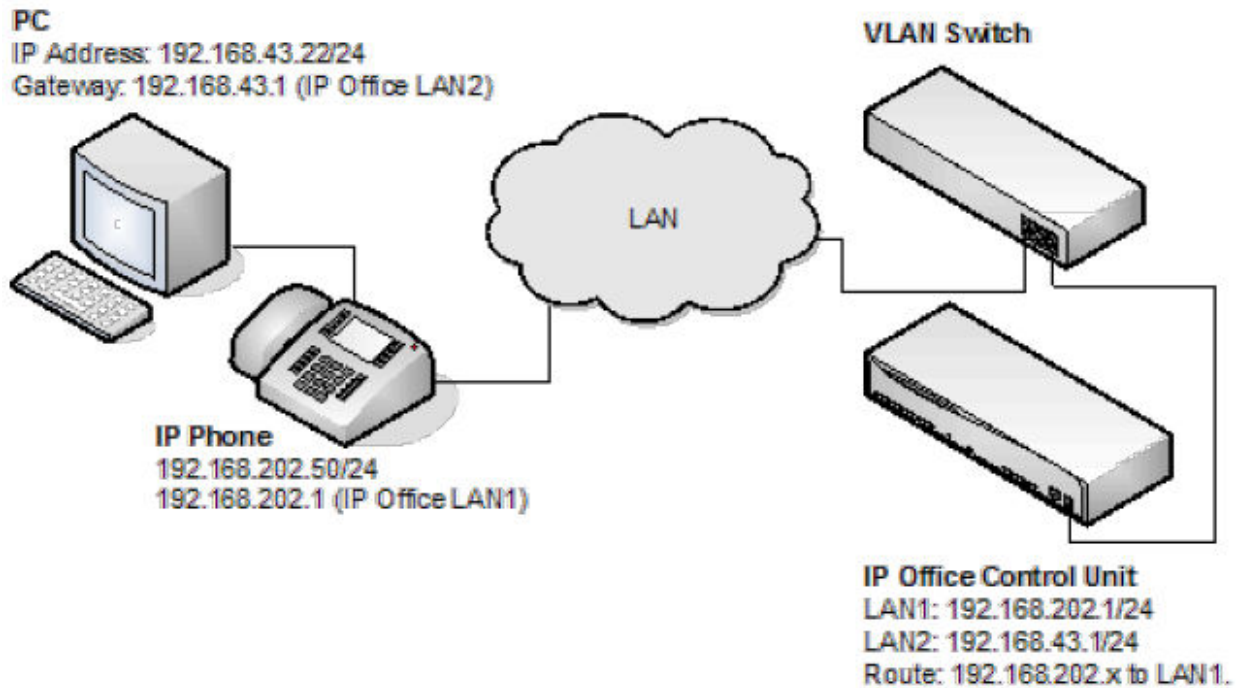
Port	VLAN 100 (VLAN vocal)	VLAN 101 (VLAN de données)	Description
3	Balisé	Non balisé	<p>Ce port a été ajouté aux VLAN 100 et VLAN 101.</p> <p><b>* Remarque :</b></p> <p>lors de l'ajout du port 3 au VLAN 100, l'option Mode doit être balisée, mais elle ne doit pas l'être lors de son ajout au VLAN 101.</p>
5	Non balisé	-	<p>Ce port est uniquement configuré sur le VLAN 100 et non sur le VLAN 101.</p> <p>L'option Mode doit être définie sur Non balisé pour le port 5 de ce VLAN.</p>
6	-	Non balisé	<p>Le port 6 est uniquement configuré sur le VLAN 101 et non sur le VLAN 100.</p> <p>L'option Mode DOIT être définie sur Non balisé pour ce VLAN.</p>

Le fonctionnement de ce réseau dépend de la fonctionnalité définie dans la documentation HP. Celle-ci appelle ce mode de fonctionnement du VLAN : **VLAN se chevauchant**.

#### Liens connexes

[Téléphones VPN distants](#) à la page 83

## Présentation d'un exemple de système



- Configuration IP Office : le tableau ci-dessous détaille la configuration requise pour IP Office. La prise en charge du balisage 802.1 par IP Office ne nécessite aucune configuration supplémentaire.

Option	Valeur
Adresse IP du LAN1	192.168.202.1
Masque IP du LAN1	255.255.255.0
Adresse IP du LAN2	192.168.43.1
Masque IP du LAN2	255.255.255.0
Routeur	192.168.202.1
Serveur d'appels	192.168.202.1

- Téléphone IP - Configuration : dans l'exemple ci-dessous, un système d'adressage IP fixe a été configuré pour le téléphone IP.

Option	Valeur
Adresse IP	192.168.202.50
Masque IP	255.255.255.0
Routeur	192.168.202.1
Serveur d'appels	192.168.202.1
VLANID	100

- Configuration du commutateur du VLAN : le tableau ci-dessous récapitule la configuration des ports et des VLAN pour le commutateur HP.

Port	VLAN 100 (VLAN vocal)	VLAN 101 (VLAN de données)
3	Balisé	Non balisé
5	Non balisé	-
6	-	Non balisé

- PC - Configuration : la configuration IP du premier ordinateur (PC1) est exposée ci-dessous. Aucune option permettant la prise en charge du balisage 802.1p ou 802.1q n'est activée sur cet ordinateur.

Option	Valeur
Adresse IP	192.168.43.22
Masque IP	255.255.255.0
Routeur	192.168.43.1

## Récapitulatif

Le port auquel l'ordinateur et le téléphone IP sont connectés permet de recevoir deux types de cadres Ethernet (qui sont envoyés à partir du téléphone ou de l'ordinateur) :

- Les paquets balisés sont envoyés par le téléphone IP.
- Les paquets non balisés sont envoyés par l'ordinateur.

Lorsque l'ordinateur rattaché au port du téléphone IP envoie un paquet non balisé, celui-ci est transmis uniquement au VLAN 101. Cela est dû au fait que lorsque le port 3 a été ajouté au VLAN 101, l'option **Mode** a été définie sur Non balisé. À l'inverse, pour l'autre VLAN (101), l'option a été définie sur **Balisé** pour le port 3 du VLAN 101. Par conséquent, les paquets balisés sont transmis au VLAN 100 tandis que les paquets non balisés sont envoyés au VLAN 101.

Les téléphones IP génèrent des paquets balisés. Comme l'option « Non balisé » est sélectionnée pour le port 5 du VLAN 100, la balise 802.1 est supprimée avant que le commutateur ne transmette le paquet à ce port. De même, lorsqu'un paquet non balisé est généré et envoyé par IP Office, le commutateur balise ce paquet avant de le transmettre au port 3 du LAN.

## Liens connexes

[Téléphones VPN distants](#) à la page 83

# Chapitre 15 : Autre configuration du serveur DHCP

La méthode d'installation recommandée pour les téléphones IP H.323 utilise un serveur DHCP. À titre d'exemple, le présent document décrit les étapes de base permettant d'utiliser un serveur Windows comme serveur DHCP dans le cadre de l'installation d'un téléphone IP. Les principes de définition d'un champ d'application s'appliquent à la plupart des serveurs DHCP.

Vous devez obtenir les informations suivantes du gestionnaire de réseau du client :

- Plage d'adresses IP et le masque de sous-réseau que les téléphones IP H.323 doivent utiliser.
- L'adresse IP de passerelle
- Le nom de domaine DNS, l'adresse du serveur DNS et l'adresse du serveur WINS
- La durée du contrat DHCP
- L'adresse IP de l'unité IP Office
- L'adresse IP du PC exécutant Manager (ce PC sert de serveur de fichiers pour les téléphones IP H.323 au cours de l'installation).

## Liens connexes

[Autres options](#) à la page 92

[Vérification de la prise en charge du serveur DHCP](#) à la page 94

[Création d'un champ d'application](#) à la page 95

[Ajout d'une option 242](#) à la page 96

[Activation du champ d'application](#) à la page 97

---

## Autres options

Dans ce document, nous avons publié toutes les informations concernant les téléphones IP jusqu'aux paramètres du champ d'application et de l'option 176 ou 242. Selon le serveur DHCP, il se peut que vous deviez utiliser d'autres options dans le champ d'application.

Option	Description
Option 1 : masque de sous-réseau	

*Le tableau continue ...*

Option	Description
Option 3 : adresse IP de la passerelle	Plusieurs adresses peuvent être définies, mais la liste complète de ces adresses ne peut contenir plus de 255 caractères ASCII. Vous devez séparer les adresses IP par des virgules, sans insérer d'espace.
Option 6 : adresse du ou des serveurs DNS	Plusieurs adresses peuvent être définies, mais la liste complète de ces adresses ne peut contenir plus de 127 caractères ASCII. Vous devez séparer les adresses IP par des virgules, sans insérer d'espace. Au moins l'une des adresses définies pour l'Option 6 doit être une adresse valide, différente de zéro, au format décimal, séparée par un point.
Option 15 : Nom du domaine DNS	Cette chaîne contient le nom du domaine à utiliser lorsque les noms DNS définis parmi les paramètres système sont convertis en adresses IP. Ce nom de domaine est ajouté au nom DNS avant que le téléphone IP ne tente de résoudre l'adresse DNS. L'Option 15 doit être définie si vous prévoyez d'utiliser un nom DNS pour le serveur HTTP.
Option 51 : Durée du contrat DHCP	<p>Si cette option n'est pas appliquée, l'offre DHCP est rejetée. Avaya conseille de définir une durée d'un minimum de six (6) semaines. Si cette option est définie sur FFFFFFFF hex, on considère que la durée du contrat pour l'adresse IP est illimitée, en vertu de l'alinéa 3.3 du document RFC 2131., Dans le cas où les Options 58 et 59 sont utilisées, il est inutile de recourir aux procédures de renouvellement et de reliaison. Lorsque les contrats arrivent à échéance, les téléphones IP Avaya redémarrent.</p> <ul style="list-style-type: none"> <li>• Il est conseillé d'octroyer suffisamment de contrats afin que l'adresse IP d'un téléphone IP ne change pas lorsqu'il est brièvement mis hors ligne.</li> <li>• Conformément à la norme DHCP, lorsqu'un contrat DHCP arrive à échéance, le périphérique doit immédiatement cesser d'utiliser l'adresse IP qui lui est attribuée. Si le réseau rencontre des difficultés et que l'unique serveur DHCP est un serveur centralisé, le téléphone ne pourra pas accéder au serveur. Dans ce cas, le téléphone est hors service jusqu'à ce que le serveur devienne à nouveau disponible.</li> <li>• Une fois qu'une adresse IP est attribuée au téléphone, celui-ci continue d'utiliser cette adresse après l'expiration du contrat, jusqu'à ce qu'un conflit avec un autre périphérique soit détecté. Le paramètre personnalisé DHCPSTD du téléphone IP de la série 1600 permet à l'administrateur de préciser si le téléphone : <ul style="list-style-type: none"> <li>- Est conforme à la norme DHCP. Dans ce cas, le paramètre DHCPSTD doit être défini sur 1 ;</li> <li>- Continue d'utiliser son adresse IP après l'expiration du bail DHCP. Dans ce cas, le paramètre DHCPSTD doit être défini sur 0. C'est l'option par défaut. Si ce paramètre est utilisé, après expiration du contrat DHCP, le téléphone envoie une requête ARP correspondant à l'adresse IP qui lui était attribuée toutes les cinq (5) secondes. La requête est répétée jusqu'à ce que le téléphone reçoive une réponse ARP. Une fois qu'il a reçu une réponse ARP, le téléphone affiche un message d'erreur, définit son adresse IP sur 0.0.0.0 et tente à nouveau de contacter le serveur DHCP.</li> </ul> </li> </ul>
Option 52 : option de surcharge	Si cette option est utilisée dans un message, le téléphone interprète les champs de nom et de fichier conformément à l'alinéa 9.3 du document IETF RFC 2132, répertorié dans l'annexe B : documentation connexe.
Option 53 : Type de message DHCP	La valeur est soit 1 (DHCPDISCOVER), soit 3 (DHCPREQUEST).

*Le tableau continue ...*

Option	Description
Option 55 : Liste de requête de paramètres	Vous pouvez saisir les valeurs suivantes : 1 (masque de sous-réseau), 3 (adresse(s) IP du routeur), 6 (adresse(s) IP du serveur des noms de domaine), 15 (nom de domaine), NVSSON (numéro d'option spécifique au site).
Option 57 : Taille maximum du message DHCP	Utilisée par un client ou un serveur DHCP pour spécifier la taille maximale du message DHCP prêt à être accepté.
Option 58 : Temps de renouvellement du contrat DHCP	Si cette option n'est pas utilisée ou si elle est définie sur une valeur supérieure à celle de l'Option 51, la valeur par défaut de T1 (compteur de renouvellement) est utilisée, en vertu de l'alinéa 4.5 du document IETF RFC 2131.
Option 59 : Temps de reliaison du contrat DHCP	Si cette option n'est pas utilisée ou si elle est définie sur une valeur supérieure à celle de l'Option 51, la valeur par défaut de T2 (compteur de reliaison) est utilisée, en vertu de l'alinéa 4.5 du document IETF RFC 2131.

**\* Remarque :**

sur les téléphones IP H.323, tous les paramètres de l'Option 66 sont annulés par toute saisie TFTP dans l'Option 176. Il peut être utile d'inclure l'Option 66 dans le champ d'application lorsque d'autres adresses du responsable de passerelle sont nécessaires dans les paramètres de l'Option 176, tout en restant dans la limite des 127 caractères.

**Liens connexes**

[Autre configuration du serveur DHCP](#) à la page 92

## Vérification de la prise en charge du serveur DHCP

### Procédure

1. Sur le serveur, sélectionnez **Démarrer > Programmes > Outils d'administration > Gestion de l'ordinateur**.
2. Sous **Services et applications**, dans l'arborescence de gestion de l'ordinateur, trouvez le protocole **DHCP**.
3. Si le protocole DHCP ne s'y trouve pas, vous devez alors installer les composants DHCP. Consultez la documentation Microsoft.

### Étapes suivantes

Si le rôle du serveur DHCP est pris en charge, la première étape consiste à créer un champ d'application pour les adresses qui seront utilisées par les téléphones IP.

**Liens connexes**

[Autre configuration du serveur DHCP](#) à la page 92

# Création d'un champ d'application

## À propos de cette tâche

Le champ d'application du DHCP définit les adresses IP que le serveur DHCP est autorisé à générer en réponse aux requêtes DHCP. Vous pouvez définir différents champs d'application pour différents types de périphériques.

## Procédure

1. Accédez à **Démarrer > Programmes > Outils d'administration > DHCP**
2. Cliquez sur le serveur avec le bouton droit et sélectionnez **Nouveau > Champ d'application**
3. L'assistant de création du champ d'application démarrera. Cliquez sur **Suivant**.
4. Saisissez un nom et un commentaire pour le champ d'application, puis cliquez sur **Suivant**.
5. Saisissez la fourchette d'adresses à utiliser, allant par exemple de 200.200.200.1 à 200.200.200.15 (rappelez-vous que la partie hôte ne peut être 0).
6. Saisissez le masque de sous-réseau comme étant le nombre de bits utilisés ou le masque réel. Par exemple, 24 correspond à la même chose que 255.255.255.0. Cliquez ensuite sur **Suivant**.
7. Vous pouvez préciser les adresses à exclure. Vous pouvez effectuer cette opération en saisissant une plage et en cliquant sur **Ajouter**.

La plage saisie doit être comprise entre 200.200.200.5 et 200.200.200.7.

### **Remarque :**

Vous devez exclure IP Office de cette plage, puisque les options DHCP dans IP Office doivent être désactivées. Il ne s'agit que d'un conseil. Une autre méthode consiste à laisser les adresses en dehors des champs d'application disponibles.

8. Cliquez sur **Suivant**.
9. Réglez la durée du contrat des adresses.
 

Si la durée est trop longue, les adresses utilisées par les périphériques qui ne sont plus rattachés n'expirent pas et ne peuvent donc pas être réutilisées dans un délai raisonnable. Cela réduit le nombre d'adresses disponibles pour de nouveaux périphériques. Si la durée est trop courte, cela crée un trafic inutile pour le renouvellement d'adresses. La durée par défaut est de 8 jours.
10. Cliquez sur **Suivant**.
11. L'assistant propose de configurer les options DHCP les plus courantes. Sélectionnez **Oui**, puis cliquez sur **Suivant**.
12. Saisissez l'adresse de la passerelle et cliquez sur **Ajouter**.
13. Cliquez sur **Suivant**.
14. Saisissez le domaine DNS (par exemple, exemple.com) et les adresses du serveur DNS, puis cliquez sur **Suivant**.
15. Saisissez les adresses du serveur WINS, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.

16. Il vous est ensuite demandé si vous souhaitez activer le champ d'application. Sélectionnez **Non**, puis cliquez sur **Suivant**.
17. Cliquez sur **Terminer**.

## Résultat

Le nouveau champ d'application est désormais répertorié et son état est **Inactif**.

Après avoir créé le champ d'application que nous souhaitons voir utilisé par les téléphones IP, un ensemble d'options doit être ajouté pour correspondre au numéro d'option spécifique au site (SSON) qui sera utilisé par les téléphones. Le SSON utilisé par défaut par les téléphones des séries 1600 et 9600 est 242.

## Liens connexes

[Autre configuration du serveur DHCP](#) à la page 92

---

# Ajout d'une option 242

## À propos de cette tâche

Outre les informations sur les adresses IP, les serveurs DHCP peuvent communiquer d'autres informations en réponse aux demandes de différents numéros d'option DHCP particuliers. Les paramètres de chaque option sont liés au champ d'application. Les téléphones IP H.323 des séries 1600 et 9600 utilisent SSON 242 pour demander des informations supplémentaires à un serveur DHCP. Cette option inclut la possibilité de définir l'adresse de l'opérateur de contrôle d'appels du téléphone H.323 (IP Office) et celle du serveur de fichiers HTTP.

## Procédure

1. Cliquez avec le bouton droit sur le serveur DHCP.
2. Dans le menu contextuel, sélectionnez **Options prédéfinies**.
3. Sélectionnez **Ajouter**.
4. Saisissez les informations suivantes :
  - a. Dans **Nom**, saisissez `16xxOptions`.
  - b. Dans **Type de données**, saisissez `String (Chaîne)`.
  - c. Dans **Code**, saisissez `242`.
  - d. Dans **Description**, saisissez `IP Phone settings (Paramètres du téléphone IP)`.
5. Cliquez sur **OK**.
6. Dans le champ de la valeur de chaîne, saisissez `MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719,HTTPSRVR=yyy.yyy.yyy.yyy,HTT  
PDIR=z, VLANTEST=0`.
  - Longueur maximum de chaîne : 127 caractères. Pour réduire la longueur, l'adresse du serveur TFTP peut être précisée en liant une entrée Option 66 au champ d'application. Reportez-vous à la section [Autres options](#) à la page 92.

`MCIPADD=` est l'adresse du responsable de passerelle H.323 (serveur d'appels). En général, il s'agit de l'adresse du réseau LAN1 de l'unité IP Office. Vous pouvez saisir

plusieurs adresses IP en les séparant toutes d'une virgule et sans espace. Cela permet de préciser le responsable de passerelle H.323 de remplacement. les téléphones attendent trois (3) minutes avant de basculer sur le responsable de remplacement et ne reviennent sur le premier serveur qu'une fois que celui-ci est réparé et que le téléphone a été redémarré.

- MCPORT=l'adresse de port RAS permettant de lancer l'enregistrement du téléphone. La valeur par défaut est 1719.
- HTTPSRVR=l'adresse IP du serveur de fichiers HTTP.
- HTTPDIR=le répertoire de fichiers HTTP dans lequel se trouvent les fichiers du téléphone IP. Cette saisie n'est pas nécessaire si ces fichiers se trouvent dans le répertoire racine du serveur.

7. Cliquez sur **OK**.
8. Développez le serveur en cliquant sur le signe [+] en regard du nom du serveur.
9. Cliquez sur le champ d'application que vous venez de créer pour les téléphones 1600 et 9600.
10. Dans le panneau de droite, cliquez avec le bouton droit sur le champ d'application et sélectionnez **Options du champ d'application**.
11. Dans l'onglet Général, assurez-vous que vous avez coché l'option 242.
12. Vérifiez que la valeur de chaîne est correcte et cliquez sur **OK**.

### Étapes suivantes

Après avoir créé une option 242 avec le champ d'application que nous souhaitons voir utilisé par les téléphones IP, nous devons ensuite activer le champ d'application.

#### Liens connexes

[Autre configuration du serveur DHCP](#) à la page 92

---

## Activation du champ d'application

Activez le champ d'application manuellement en cliquant avec le bouton droit sur le champ d'application, puis sélectionnez **Toutes les tâches et Activer**. L'activation est immédiate.

Vous pourrez alors démarrer l'installation des téléphones IP H.323 à l'aide du protocole DHCP. Si vous utilisez Manager en tant que serveur HTTP ou TFTP, vérifiez que celui-ci est bien en cours d'exécution sur le PC correspondant.

#### Liens connexes

[Autre configuration du serveur DHCP](#) à la page 92

# Chapitre 16 : Prise en charge du protocole SRTP

Pour IP Office version 9.1, le protocole SRTP est pris en charge.

- Modes IP Office pris en charge : le SRTP est pris en charge dans tous les modes IP Office.
- Téléphones pris en charge : la prise en charge peut être appliquée aux postes SIP et H323. Cependant, certaines restrictions peuvent s'appliquer à certains modèles particuliers de téléphone IP.
  - Pris en charge pour H323 par les téléphones 9608, 9611, 9621 et 9641.
  - Pris en charge pour SIP sur les téléphones Avaya et tiers.
- Lignes réseau prises en charge : la prise en charge peut être appliquée à tous les types de lignes IP (SIP, SM et IP Office (SCN)), à l'exception des lignes réseau H323 externes.
- Licences et capacité : l'utilisation du protocole SRTP ne nécessite aucune licence ni aucun abonnement. Cependant, l'utilisation du protocole SRTP impacte la capacité d'appel du système.
  - Sur les systèmes IP500 V2/IP500 V2A dotés d'une carte VCM IP500, cette dernière est utilisée pour prendre en charge le protocole SRTP et réduire l'impact sur la capacité d'appel du système. Ceci ne s'applique pas aux cartes combinées.

## Liens connexes

[Activation du protocole SRTP au niveau du système](#) à la page 98

[Support direct](#) à la page 100

---

## Activation du protocole SRTP au niveau du système

Par défaut, l'ensemble des postes et des lignes IP sont configurés de manière à reproduire les paramètres systèmes du plus haut niveau pour le protocole SRTP, qui sont activées ou désactivées. Cette approche simplifie l'activation de SRTP en garantissant que l'ensemble des périphériques utilise les mêmes paramètres SRTP. Grâce à cette approche, une fois que SRTP est activé, la seule configuration requise sur les périphériques est de désactiver SRTP sur les périphériques ou les lignes qui n'ont pas besoin de l'utiliser.

Les lignes SIP constituent toutefois une exception à la règle ci-dessus, puisque SRTP est désactivé par défaut sur celles-ci. Cela est dû au fait le nombre de fournisseurs de lignes SIP prenant actuellement en charge SRTP. Cependant, si nécessaire, il est possible de configurer les lignes SIP pour que leurs paramètres soient identiques à ceux du système.

**Liens connexes**

[Prise en charge du protocole SRTP](#) à la page 98

[Activation du protocole SRTP au niveau du système](#) à la page 99

[Désactivation du protocole SRTP sur un poste ou une ligne](#) à la page 99

---

## Activation du protocole SRTP au niveau du système

**Procédure**

1. Récupérez la configuration du système.
2. Cliquez sur **Système** et sélectionnez l'onglet **Sécurité VoIP**.
3. Pour **Protection du média**, sélectionnez le niveau de fonctionnement STRP requis :

Paramètre	Description
<b>Désactivé</b>	Le protocole SRTP n'est pas utilisé pour les connexions.
<b>Du mieux possible</b>	Prend en charge les protocoles RTP et SRTP. Utilisez SRTP si des paramètres SRTP identiques peuvent être négociés avec l'extrémité distante. Pour ce faire, l'extrémité distante doit prendre en charge srtp rfc5939 (négociation de la capacité de SRTP). Sinon, utilisez RTP. Veuillez noter que les téléphones E129 ne prennent pas en charge <b>Du mieux possible</b> .
<b>Appliqué</b>	Utilise uniquement le protocole SRTP. L'appel n'est pas autorisé si la partie distante ne prend pas en charge le même protocole SRTP.
<b>Paramètres avancés</b>	Si vous avez sélectionné <b>Du mieux possible</b> ou <b>Appliqué</b> comme méthode STRP, il est recommandé de conserver la valeur par défaut de tous les autres paramètres SRTP.  Les paramètres par défaut de l'ensemble des cryptogrammes et balises SRTP ont été choisis de manière à fonctionner avec tous les dispositifs Avaya H323 et SIP. Par exemple, la majorité des implémentations Avaya ne prennent pas en charge le chiffage RTCP tandis que les téléphones Avaya H323 prennent uniquement en charge l'ensemble de paramètres cryptographiques SHA_80.

4. Cliquez sur **OK**.

**Liens connexes**

[Activation du protocole SRTP au niveau du système](#) à la page 98

---

## Désactivation du protocole SRTP sur un poste ou une ligne

**Procédure**

1. Cliquez sur **Poste** ou **Ligne** puis sélectionnez le poste ou la ligne souhaités.
2. Sélectionnez l'onglet **VoIP**.
3. Définissez le paramètre **Protection du média** sur **Désactivé**.
4. Cliquez sur **OK**.

## Étapes suivantes

Répétez ce processus pour toute autre extension ou ligne pour laquelle SRTP ne devrait pas être utilisé.

### Liens connexes

[Activation du protocole SRTP au niveau du système](#) à la page 98

---

## Support direct

Si l'acheminement direct est configuré, le système tente de négocier un acheminement direct entre les deux parties de l'appel. Si le protocole SRTP est utilisé, en plus de vérifier la présence de critères VoIP correspondants (par exemple, la prise en charge des mêmes codecs), le système vérifie également la présence de paramètres identiques de protection du média et de protection avancée du média (séries de balises et paramètres cryptographiques SRTP). Toute incompatibilité empêche l'utilisation de l'acheminement direct.

Les appels entre différents tronçons d'appel définis sur différents niveaux de **Protection du média** (**Désactivé**, **Du mieux possible** ou **Appliqué**) n'utiliseront pas de support direct.

### Liens connexes

[Prise en charge du protocole SRTP](#) à la page 98

# Chapitre 17 : Prise en charge du protocole TLS

Pour les versions 10 et ultérieures d'IP Office, il est possible d'utiliser TLS pour la connexion des téléphones 9600. Lorsqu'il est activé, TLS est utilisé pour le RAS TCP et pour la signalisation d'appel entre le téléphone et le système IP Office.

- Le protocole TLS est pris en charge par les modèles 9608, 9611, 9621 et 9641.
- Le téléphone doit exécuter le firmware 6.6029 ou une version supérieure.
- Le téléphone doit également utiliser un mot de passe CRAFT qui n'est pas le mot de passe par défaut.
- Vous pouvez configurer l'utilisation de TLS par le système comme facultative ou imposée.

## Récapitulatif de la procédure

1. Personnalisez le mot de passe de processus CRAFT.
2. Ajoutez le certificat d'identité.
3. Activer TLS sur le système IP Office
4. Activez TLS sur le téléphone.

## Remarques complémentaires

Pour les téléphones utilisant TLS :

- La connexion au serveur de fichiers HTTPS utilise le port 8411. Le serveur de fichiers doit utiliser le même certificat.
- Si l'extrémité distante utilise également SRTP, le téléphone utilise le port 8443 pour la sauvegarde/restauration.

## Liens connexes

[Modification du mot de passe CRAFT](#) à la page 102

[Ajout du certificat d'identité](#) à la page 102

[Téléchargement du certificat d'identité à partir d'un serveur Linux](#) à la page 103

[Chargement d'un certificat dans le magasin de certificats approuvés du serveur](#) à la page 103

[Activation de TLS sur le système IP Office](#) à la page 104

[Activation de TLS sur les téléphones](#) à la page 104

[Vérification du fonctionnement de TLS](#) à la page 105

---

## Modification du mot de passe CRAFT

### À propos de cette tâche

Le fonctionnement TLS du téléphone ne peut pas être modifié/activé si les téléphones utilisent le mot de passe de processus CRAFT défini par défaut. Le mot de passe peut être modifié comme suit :

### Procédure

1. Si les téléphones téléchargent un fichier `46xxsettings.txt` depuis un serveur de fichiers, procédez comme suit :
  - a. Ajoutez une entrée **DÉFINIR PROCPSWD** au fichier `46xxsettings.txt`, suivie du mot de passe à utiliser.
  - b. Redémarrez les téléphones pour charger les nouveaux paramètres.
2. Si les téléphones utilisent les paramètres générés automatiquement par IP Office :
  - a. Recevez la configuration d'IP Office et localisez l'utilisateur **Aucun utilisateur**.
  - b. Dans l'onglet **Numéros source**, ajoutez **SET\_46xx\_PROCPSWD** suivi du nouveau mot de passe.

Notez que cette commande est sensible à la casse.
  - c. Enregistrez la configuration et redémarrez le système.
3. Pour afficher le paramètre de fichier généré automatiquement :
  - a. Ouvrez le navigateur et saisissez `http://<server_address>/46xxsettings.txt`.
  - b. Dans le fichier, insérez une ligne commençant par **DÉFINIR PROCPSWD**, suivie du nouveau mot de passe.

### Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

## Ajout du certificat d'identité

Par défaut, le certificat IP Office racine est utilisé. Pour un système IP500 V2, il s'agit de son propre certificat de sécurité autosigné et aucune modification supplémentaire n'est requise. Pour les serveurs Linux, il convient de télécharger le certificat autosigné du serveur, puis de charger ce certificat sur le magasin de certificats approuvés du service IP Office.

Si vous souhaitez utiliser un certificat tiers, vous devez également charger celui-ci sur le magasin de certificats approuvés d'IP Office.

Le téléphone est informé du certificat qu'il doit utiliser par un paramètre dans le fichier `46xxsettings.txt` qu'il reçoit. Les paramètres suivants sont utilisés :

- `SET TLSSRVRVERIFYID 1` : ce paramètre ordonne au téléphone de vérifier le certificat TLS.
- `SET TRUSTCERTS Root-CA-xxxxxxxxx.pem` : ce paramètre indique le nom du certificat de sécurité que le téléphone doit demander et charger lorsqu'il démarre.

Lorsqu'IP Office reçoit une demande de certificat, il effectue une recherche dans son magasin de certificats approuvés. Si les octets 13 à 16 de la clé publique du certificat AC racine correspondent à la section xxxxxxxx du nom de fichier demandé, IP Office fournit alors le certificat AC racine en tant que fichier généré automatiquement nommé `Root-CA-xxxxxxx.pem`.

Pour les systèmes utilisant des fichiers autogénérés, les paramètres sont ajoutés automatiquement. Pour les autres installations, les paramètres doivent être ajoutés manuellement à la section du fichier 46xxsettings destinée aux téléphones 9608, 9611, 9621 et 9641.

#### Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

## Téléchargement du certificat d'identité à partir d'un serveur Linux

### À propos de cette tâche Procédure

1. Rendez-vous sur [https://%3Cserver\\_address%3E:7071](https://%3Cserver_address%3E:7071) et connectez-vous aux menus Web Control du serveur.  
  
Vous pouvez également vous connecter aux menus de gestion Web du serveur, puis sélectionner **Affichage de la plateforme**.
2. Sélectionnez l'onglet **Paramètres**, puis **Général**.
3. Recherchez la section **Certificats**.
4. Dans la section **Paramètres de l'autorité certifiée**, cliquez sur **Télécharger (encodé en PEM)**.

#### Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

## Chargement d'un certificat dans le magasin de certificats approuvés du serveur

### Procédure

1. Démarrez IP Office Manager.
2. Sélectionnez **Fichier > Options avancées > Paramètres de Sécurité**.
3. Sélectionnez le serveur et connectez-vous.
4. Sélectionnez **Système**.
5. Sélectionnez l'onglet **Certificats**.

6. Dans la section **Magasin de certificats approuvés**, cliquez sur **Ajouter**.

#### Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

## Activation de TLS sur le système IP Office

### À propos de cette tâche

Le système IP Office peut utiliser un certain nombre d'options TLS.

### Procédure

1. Utilisez IP Office Manager pour charger la configuration du serveur.
2. Sélectionnez **Système**.
3. Sélectionnez l'onglet **LAN1** ou **LAN2**, selon vos besoins, puis sélectionnez l'onglet **VoIP**.
4. L'opération TLS est contrôlée par le champ **Signalisation H.323 par TLS**. Sélectionnez le mode TLS souhaité :
  - **Désactivé** : ne pas utiliser TLS. Les téléphones configurés pour TLS reviennent à une connexion TCP normale.
  - **Préféré** : cette option vous permet d'utiliser TLS avec les téléphones configurés pour TLS, mais elle permet également des connexions TCP normales depuis d'autres téléphones.
  - **Appliqué** : nécessite TLS. Les connexions des téléphones non configurés pour TLS seront refusées. Veuillez noter que lorsque cette option est sélectionnée, le **Port de signalisation d'appel distant** est défini sur 1300.
5. Cliquez sur **OK**.
6. Enregistrez les modifications apportées à la configuration et laissez le système redémarrer.

#### Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

## Activation de TLS sur les téléphones

### À propos de cette tâche

Pour accéder au paramètre TLS pour les téléphones, utilisez le menu Débogage.

#### \* Remarque :

Lorsqu'un téléphone existant est mis à niveau avec un microprogramme compatible TLS, la valeur par défaut du paramètre H.323 Signalisation par TLS devient « Activé ». Toutefois, sur les systèmes qui ne sont pas configurés pour l'utilisation de TLS, les téléphones continuent d'utiliser une connexion TCP normale.

## Procédure

1. Appuyez sur **MUET**, puis sur mot de passe de processus CRAFT et enfin sur #.  
Vous pouvez accéder à ce menu sur les téléphones à l'aide du mot de passe de processus CRAFT défini par défaut. Cependant, dans ce cas, vous pouvez uniquement afficher les paramètres mais vous ne pouvez pas les modifier.
2. Faites défiler l'écran et sélectionnez **DÉBOGAGE**.
3. Faites défiler jusqu'à **Signalisation H.323 par TLS**.
4. Modifiez le paramètre selon vos besoins.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Quitter**.

## Résultat

Le téléphone redémarre en utilisant le nouveau paramètre.

## Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

---

# Vérification du fonctionnement de TLS

Il est possible de vérifier et de confirmer l'utilisation de TLS de la manière suivante.

- System Status Application : les détails du **Poste** indiquent que le **Protocole de couche 4** est utilisé par la connexion du poste. **TLS** s'affiche lorsque TLS est utilisé.
- System Monitor : dans le Monitor, sélectionnez **État > État du téléphone H323**. La colonne **Transport** affiche **TLS** pour les postes utilisant TLS pour leur connexion.

Dans le suivi de Monitor, les enregistrements H323 RAS Tx et Rx indiquent si les postes utilisent TLS. De la même manière, les enregistrements H323 CS et RAS indiquent l'utilisation du port 1300.

## Liens connexes

[Prise en charge du protocole TLS](#) à la page 101

# Partie 5 : Divers

# Chapitre 18 : Options d'administration statique

Il est possible de modifier plusieurs paramètres par le biais du téléphone après son installation. Utilisez ces procédures uniquement si vous installez des adresses statiques. N'utilisez pas ces procédures si vous utilisez le serveur DHCP, excepté si vous tentez de réaffecter un téléphone qui avait été précédemment installé de manière statique.

Pour configurer les paramètres de tous les téléphones IP H.323 d'un système, vous pouvez modifier le fichier de script `46xxsettings.txt`. Toutefois, les valeurs attribuées par l'intermédiaire de l'administration statique prennent le pas sur celles qui sont définies dans le fichier `46xxsettings.txt`. Elles restent actives pour le téléphone IP jusqu'à ce qu'un nouveau fichier d'amorçage soit téléchargé.

## Liens connexes

[Utilisation des options d'administration statique](#) à la page 107

[Mot de passe de processus administrateur](#) à la page 109

[Activation de l'interface du concentrateur](#) à la page 109

[Affichage des détails du téléphone](#) à la page 111

[Procédure de test automatique pour les téléphones de la série 1600](#) à la page 113

[Procédure de test automatique pour les téléphones de la série 9600](#) à la page 114

[Réinitialisation d'un téléphone](#) à la page 114

[Désactivation d'un téléphone](#) à la page 115

[Numéro d'option spécifique au site](#) à la page 116

---

## Utilisation des options d'administration statique

La méthode utilisée pour accéder à l'administration statique dépend du type de téléphone utilisé. Vous pouvez accéder à la plupart des fonctions d'administration statique en utilisant une séquence de touches qui commence soit par la touche **MUET** soit par la touche **MISE EN ATTENTE**. Les versions récentes du micrologiciel font plus souvent appel à la touche **MUET**, mais certains téléphones, comme ceux de la série 1600, prennent uniquement en charge l'utilisation de la touche **MUET**.

## Liens connexes

[Options d'administration statique](#) à la page 107

[Saisie des options administratives sur les téléphones de la série 1600](#) à la page 108

[Saisie des options administratives sur les téléphones de la série 9600](#) à la page 108

---

## Saisie des options administratives sur les téléphones de la série 1600

### À propos de cette tâche

Cette section décrit la façon de saisir des données pour les options administratives.

### Procédure

1. Lorsque le téléphone est inactif, appuyez sur **MUET**.  
Une fois que vous avez appuyé sur **MUET**, si vous n'appuyez pas sur un bouton valide dans les 6 secondes suivantes, les chiffres enregistrés sont effacés et le téléphone redevient inactif.
2. Composez le mot de passe du processus administratif.
3. Composez les chiffres de la commande requise, suivis de #.
  - Les tentatives de saisie de données non valides sont rejetées et le téléphone émet un bip d'erreur.
  - Si un chiffre est saisi pour une valeur, un champ d'adresse IP ou un masque de sous-réseau après la saisie d'un zéro, le nouveau chiffre remplace ce zéro.
  - Pour passer à l'étape suivante, appuyez sur #.

### Liens connexes

[Utilisation des options d'administration statique](#) à la page 107

---

## Saisie des options administratives sur les téléphones de la série 9600

### À propos de cette tâche

Les procédures administratives des téléphones de la série 9600 sont uniquement accessibles en redémarrant le téléphone.

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur `MUTE <password> #`.
2. Faites défiler le menu sur l'action souhaitée pour la sélectionner.  
Une fois la procédure sélectionnée terminée, le téléphone revient au menu des procédures.
3. Une fois que toutes les procédures requises sont terminées, appuyez sur **Quitter**.

### Résultat

Le téléphone redémarre avec de nouveaux paramètres.

### Liens connexes

[Utilisation des options d'administration statique](#) à la page 107

---

## Mot de passe de processus administrateur

### À propos de cette tâche

Les processus d'administration des téléphones sont protégés par l'utilisation d'un mot de passe de processus, également connu sous le nom de mot de passe CRAFT. Vous pouvez modifier la valeur par défaut de ce mot de passe en indiquant une nouvelle valeur dans le fichier `46xxsettings.txt`.

### Procédure

1. Si les téléphones téléchargent un fichier `46xxsettings.txt` depuis un serveur de fichiers, procédez comme suit :
  - a. Ajoutez une entrée **DÉFINIR PROCPSWD** au fichier `46xxsettings.txt`, suivie du mot de passe à utiliser.
  - b. Redémarrez les téléphones pour charger les nouveaux paramètres.
2. Si les téléphones utilisent les paramètres générés automatiquement par IP Office :
  - a. Recevez la configuration d'IP Office et localisez l'utilisateur **Aucun utilisateur**.
  - b. Dans l'onglet **Numéros source**, ajoutez **SET\_46xx\_PROCPSWD** suivi du nouveau mot de passe.

Notez que cette commande est sensible à la casse.
  - c. Enregistrez la configuration et redémarrez le système.
3. Pour afficher le paramètre de fichier généré automatiquement :
  - a. Ouvrez le navigateur et saisissez `http://<server_address>/46xxsettings.txt`.
  - b. Dans le fichier, insérez une ligne commençant par **DÉFINIR PROCPSWD**, suivie du nouveau mot de passe.

### Liens connexes

[Options d'administration statique](#) à la page 107

---

## Activation de l'interface du concentrateur

De nombreux téléphones IP Avaya sont dotés de l'interface du concentrateur, qui peut être utilisée pour la connexion PC de l'utilisateur. L'interface du concentrateur est activée par défaut.

### Liens connexes

[Options d'administration statique](#) à la page 107

[Activation de l'interface du concentrateur pour les téléphones de la série 1600](#) à la page 110

[Activation de l'interface du concentrateur pour la série 9600](#) à la page 110

---


## Activation de l'interface du concentrateur pour les téléphones de la série 1600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur `MUTE <password> INT #` ou `MUTE <password> 468 #`.

Les paramètres de port des téléphones s'affichent les uns après les autres. Les options varient selon les différents modèles de téléphone.

- PHY2=

Il s'agit de la prise LAN de connexion du PC, signalée par le symbole  sur le téléphone. Appuyez sur 1 ou 0 pour respectivement activer ou désactiver l'interface du concentrateur. Pour continuer, appuyez sur la touche #.

- IR=

Il s'agit du port infrarouge (IR) situé à l'avant de certains téléphones IP H.323. Appuyez sur 1 ou 0 pour respectivement activer ou désactiver l'interface du concentrateur. Pour continuer, appuyez sur la touche #.

2. Pour enregistrer les nouvelles valeurs, appuyez sur #.

### Résultat

Le message `New values being saved` (Nouvelles valeurs enregistrées) s'affichent, puis l'ensemble du téléphone revient à un fonctionnement normal.

### Liens connexes

[Activation de l'interface du concentrateur](#) à la page 109

---

## Activation de l'interface du concentrateur pour la série 9600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur `MUTE <password> #`.
2. Faites défiler le menu jusqu'à **INT**.
3. Sélectionnez le port que vous souhaitez ajuster. Les options sont **Ethernet** et **Ethernet PC**.
4. Utilisez les boutons < et > pour naviguer parmi les paramètres possibles du port.  
L'option supplémentaire **Désactivé** est proposée pour le port PC Ethernet.
5. Appuyez sur **Enregistrer**.
6. Sélectionnez une autre procédure ou appuyez sur **Quitter** pour redémarrer le téléphone.

### Liens connexes

[Activation de l'interface du concentrateur](#) à la page 109

## Affichage des détails du téléphone

Vous pouvez afficher un certain nombre de détails du téléphone. Il s'agit d'un ajout aux autres options d'adresse statique et d'administration locale qui permettent également d'examiner les paramètres.

### Liens connexes

[Options d'administration statique](#) à la page 107

[Affichage des détails des téléphones de la série 1600](#) à la page 111

[Affichage des détails des téléphones de la série 9600](#) à la page 112

## Affichage des détails des téléphones de la série 1600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur `MUTE CRAFT VIEW #` ou `MUTE 27238 8439 #`.
2. À tout moment, vous pouvez afficher les informations en appuyant sur la touche `*`. Les paramètres suivants s'affichent :

Valeur	Description
<b>Modèle</b>	Indique la référence du modèle de téléphone comme par exemple 4624D02A.
<b>Marché</b>	Affiche 1 pour export ou 0 pour national (États-Unis). Ne s'affiche pas sur tous les modèles.
<b>Numéro de série du téléphone</b>	Indique le numéro de série du téléphone.
<b>Numéro de série du PWB</b>	Indique le <b>numéro de série du tableau de connexion imprimé</b> du téléphone.
<b>Comcode du PWB</b>	Affiche le comcode du PWB.
<b>Adresse MAC</b>	Indique l'adresse MAC du téléphone sous la forme de paires de numéros hexadécimaux.
<b>Balilage L2</b>	Indique si le balilage L2 est défini sur <b>activé</b> , <b>désactivé</b> ou sur <b>automatique</b> .
<b>ID de VLAN</b>	Utilisé pour le téléphone. La valeur par défaut est 0.
<b>Adresse IP</b>	Adresse IP attribuée au téléphone.
<b>Masque de sous-réseau</b>	Masque de sous-réseau attribué au téléphone.
<b>Routeur</b>	Adresse du routeur attribuée au téléphone.
<b>Serveur de fichiers</b>	Adresse du serveur de fichiers attribué au téléphone.
<b>Serveur d'appels</b>	Adresse du responsable de passerelle du téléphone H.323.
<b>802.1X</b>	Paramètre actuel défini pour le fonctionnement du balilage 802.1X s'il est activé.

*Le tableau continue ...*

Valeur	Description
<b>Groupe</b>	Affiche le groupe défini pour ce téléphone. Les groupes permettent de déterminer quelles options le téléphone télécharge (en ce qui concerne le micrologiciel et les paramètres).
<b>Protocole</b>	Afficher <b>par défaut</b> .
<b>filename1</b>	Indique le nom du fichier d'application du téléphone dans la mémoire du téléphone. Ces valeurs proviennent du fichier d'amorçage chargé et non pas du nom du fichier réel.
<b>Ethernet 10 Mbit/s</b> <b>Ethernet 100 Mbit/s</b>	Indique la vitesse de la connexion LAN détectée.
<b>filename2</b>	Affiche le nom et le niveau du fichier de d'amorçage. Ces valeurs proviennent du fichier d'amorçage chargé et non pas du nom du fichier réel.

3. Pour mettre fin à cette procédure et revenir à l'interface utilisateur telle qu'elle était auparavant, appuyez sur la touche #.
4. Pour afficher la valeur suivante, appuyez sur la touche \*.

#### Liens connexes

[Affichage des détails du téléphone](#) à la page 111

## Affichage des détails des téléphones de la série 9600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur MUTE <password> #.
2. Faites défiler le menu jusqu'à **AFFICHAGE**, puis démarrez la procédure.

Valeur	Description
<b>Modèle</b>	Indique la référence du modèle de téléphone, par exemple 4624D02A.
<b>Numéro de série du téléphone</b>	Indique le numéro de série du téléphone.
<b>Numéro de série du PWB</b>	Indique le <b>numéro de série du tableau de connexion imprimé</b> du téléphone.
<b>Comcode du PWB</b>	Affiche le comcode du PWB.
<b>MAC</b>	Indique l'adresse MAC du téléphone sous la forme de paires de numéros hexadécimaux.
<b>Groupe</b>	Affiche le groupe défini pour ce téléphone. Les groupes permettent de déterminer quelles options le téléphone télécharge (en ce qui concerne le micrologiciel et les paramètres).
<b>Protocole</b>	Afficher <b>par défaut</b> .
<b>Fichier d'application</b>	Indique le nom du fichier d'application du téléphone dans la mémoire du téléphone. Ces valeurs proviennent du fichier d'amorçage chargé et non pas du nom du fichier réel.
<b>Ethernet</b>	Indique la vitesse de la connexion LAN détectée.

*Le tableau continue ...*

Valeur	Description
<b>Fichier de démarrage</b>	Affiche le nom et le niveau du fichier de démarrage. Ces valeurs proviennent du fichier de démarrage chargé et non pas du nom du fichier réel.
<b>Serveur proxy</b>	Affiche les détails du serveur proxy sélectionné.
<b>Fichier langue voix</b>	Nom du fichier de langue utilisé par le téléphone. Il est vide si la langue par défaut du téléphone (anglais) est utilisée.

- Appuyez sur **Retour**.
- Sélectionnez une autre procédure ou appuyez sur **Quitter** pour redémarrer le téléphone.

### Liens connexes

[Affichage des détails du téléphone](#) à la page 111

---

## Procédure de test automatique pour les téléphones de la série 1600

### Procédure

- Pour démarrer la procédure de test automatique du téléphone IP, appuyez sur MUTE <password> TEST # ou MUTE <password> 8378 #.

Le téléphone effectue les opérations suivantes :

- Chaque colonne de DEL de boutons programmables s'allume pendant une demi-seconde de gauche à droite sur le téléphone, de façon répétée. La DEL Haut-parleur/ Secret ainsi que la DEL de message en attente s'allument également l'une après l'autre.
- Les touches (autres que #) émettent un clic lorsque vous appuyez dessus.
- Les téléphones dotés d'un écran affichent le message `Self test #=end(Test automatique #=fin)` pendant une seconde une fois le test automatique démarré. Ensuite, un caractère bloc (tous les pixels) s'affiche pendant 5 secondes sur tous les emplacements de caractères affichables. L'affichage du caractère bloc permet de trouver les mauvais pixels d'affichage.
- Si le test automatique est réussi :
 

```
Self test passed
#=end
```
- Si le test automatique échoue :
 

```
Self test failed
#=end
```

- Pour terminer le test automatique, appuyez sur la touche #.

### Résultat

Le téléphone revient à un fonctionnement normal.

## Liens connexes

[Options d'administration statique](#) à la page 107

---

# Procédure de test automatique pour les téléphones de la série 9600

## Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur MUTE <password> #.
2. Faites défiler le menu jusqu'à **Test**.
3. Appuyez à nouveau sur **Test** pour confirmer l'action.

## Liens connexes

[Options d'administration statique](#) à la page 107

---

# Réinitialisation d'un téléphone

La réinitialisation d'un téléphone réinitialise toutes les valeurs système ainsi que la plupart des valeurs d'initialisation du système. Cette procédure n'a aucune répercussion sur les données et paramètres spécifiés par l'utilisateur (par ex., les données de contact, les paramètres des options, le poste ou le mot de passe de connexion, etc.). Pour supprimer toutes ces données, consultez la section [Désactivation d'un téléphone](#) à la page 115.

## Liens connexes

[Options d'administration statique](#) à la page 107

[Réinitialisation d'un téléphone de la série 1600](#) à la page 114

[Réinitialisation du téléphone de la série 9600](#) à la page 115

---

# Réinitialisation d'un téléphone de la série 1600

## Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur la séquence suivante MUTE <password> RESET #.

MUTE <password> 73738 #



### **Avertissement :**

Si vous appuyez sur la touche #, toutes les informations statiques sont immédiatement effacées, sans aucune possibilité de récupérer les données.

2. Pour continuer, appuyez sur #.

Pendant que les valeurs du système sont réinitialisées et reviennent à leurs valeurs par défaut, le message Réinitialisation des valeurs s'affiche.

Dès que les valeurs du système sont réinitialisées, le message `Redémarrer le téléphone ?` s'affiche.

3. Pour terminer la procédure sans redémarrer le téléphone, appuyez sur \*.
4. Pour redémarrer le téléphone, appuyez sur #.

La suite de la procédure dépend de l'état des fichiers d'amorçage et d'application. Reportez-vous à la section [Scénarios de redémarrage](#) à la page 118.

#### Liens connexes

[Réinitialisation d'un téléphone](#) à la page 114

## Réinitialisation du téléphone de la série 9600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur `MUTE <password> #`.
2. Faites défiler le menu, puis sélectionnez **Réinitialiser les valeurs**.
3. Appuyez sur **Réinitialiser** pour confirmer l'action.

### Résultat

Les paramètres utilisateur du téléphone sont réinitialisés et celui-ci redémarre.

#### Liens connexes

[Réinitialisation d'un téléphone](#) à la page 114

## Désactivation d'un téléphone

Le rétablissement de toutes les valeurs d'initialisation système par défaut et la suppression de l'ensemble des données spécifiques à l'utilisateur sont principalement destinés à la réparation et sont utilisés lorsque le téléphone est donné à un nouvel utilisateur. Le téléphone retrouve quasiment son état d'origine. Le téléphone conserve cependant les fichiers du firmware qui ont déjà été téléchargés.

### Remarque :

Certains paramètres, tels que les clics de boutons, les tonalités d'erreur et la sonnerie personnalisée peuvent être configurés pour un utilisateur spécifique via le MENU. Ces paramètres utilisateur seront restaurés lorsque vous enregistrez l'utilisateur sur le téléphone car ces paramètres sont configurés dans IP Office. Tous les autres paramètres (par exemple, données de contact, paramètres des options, etc.) sont effacés du téléphone.

#### Liens connexes

[Options d'administration statique](#) à la page 107

[Désactivation des téléphones de la série 1600](#) à la page 116

[Désactivation des téléphones de la série 9600](#) à la page 116

---

## Désactivation des téléphones de la série 1600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur la séquence suivante MUTE  
<password> CLEAR #.  
MUTE <password> 25327 #
2. Pour continuer, appuyez sur #.

### **Avertissement :**

Si vous appuyez sur la touche #, toutes les informations statiques sont immédiatement effacées, sans aucune possibilité de récupérer les données.

Pendant que les valeurs du système sont réinitialisées et reviennent à leurs valeurs par défaut, le message `Suppression des valeurs` s'affiche.

### Résultat

Une fois que toutes les valeurs sont effacées, le téléphone redémarre et se présente comme s'il s'agissait d'un nouveau téléphone.

### Liens connexes

[Désactivation d'un téléphone](#) à la page 115

---

## Désactivation des téléphones de la série 9600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur MUTE <password> #.
- 2.
3. Faites défiler le menu, puis sélectionnez **Effacer**.
4. Appuyez à nouveau sur **Effacer** pour confirmer l'action.

### Résultat

Les paramètres du téléphone sont effacés et celui-ci redémarre.

### Liens connexes

[Désactivation d'un téléphone](#) à la page 115

---

## Numéro d'option spécifique au site

Les téléphones IP utilisent le numéro d'option spécifique au site (SSON) pour demander des informations auprès d'un serveur DHCP qui est spécifiquement dédié aux téléphones et non pas aux autres périphériques IP pris en charge par le serveur DHCP. Ce numéro doit correspondre au numéro d'un groupe d'options du serveur DHCP qui définit les différents paramètres à définir pour le téléphone.

Le SSON par défaut utilisé par les téléphones Avaya des séries 1600 et 9600 est 242. Pour les téléphones pris en charge par le serveur DHCP d'IP Office, le SSON utilisé par le téléphone doit correspondre à l'un des numéros d'options spécifiques au site définis dans la configuration IP Office.

 **Avertissement :**

N'appliquez pas cette procédure si vous utilisez des adresses statiques. N'exécutez cette procédure que dans le cadre d'adresses DHCP et si le numéro d'option DHCP diffère du numéro initial par défaut.

#### Liens connexes

[Options d'administration statique](#) à la page 107

[SSON sur les téléphones de la série 1600](#) à la page 117

[SSON sur les téléphones de la série 9600](#) à la page 117

---

## SSON sur les téléphones de la série 1600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur MUTE <password> SSON # ou MUTE <password> 7766 #

**SSON=** s'affiche, suivi de la valeur correspondante actuelle.

2. Saisissez le nouveau paramètre. Il doit s'agir d'un nombre compris entre 128 et 255.
3. Pour annuler cette procédure, appuyez sur \* ou sur # pour enregistrer la nouvelle valeur.

#### Liens connexes

[Numéro d'option spécifique au site](#) à la page 116

---

## SSON sur les téléphones de la série 9600

### Procédure

1. Lorsque le téléphone est raccroché et inactif, appuyez sur MUTE <password> #.
2. Faites défiler le menu jusqu'à **SSON**, puis démarrez la procédure.
3. Saisissez le nouveau numéro SSON que le téléphone devra utiliser à son prochain démarrage.
4. Appuyez sur **Enregistrer**.
5. Sélectionnez une autre procédure ou appuyez sur **Quitter** pour redémarrer le téléphone.

#### Liens connexes

[Numéro d'option spécifique au site](#) à la page 116

# Chapitre 19 : Scénarios de redémarrage

La séquence de la procédure de redémarrage varie en fonction de la version du fichier d'amorçage du téléphone déjà téléchargée sur celui-ci ainsi que des versions figurant sur le serveur de fichiers. Cette annexe explique les différents scénarios possibles.

Toutes les procédures de démarrage suivantes impliquent les mêmes étapes initiales lorsque le téléphone négocie avec le serveur DHCP et le serveur de fichiers.

1. Une fois alimenté, le téléphone affiche `Redémarrage en cours`, puis `Initialisation en cours`
2. Pendant que le fichier d'application (s'il existe) ou le code d'amorçage est décompressé dans la mémoire vive (RAM), le téléphone affiche le message `Chargement`. Comme ceci prend un certain temps, des astérisques, des points puis à nouveau des astérisques s'affichent sur la deuxième ligne pour indiquer une activité.
3. Lorsque le code de la RAM prend le contrôle, le message `Démarrage` s'affiche.
4. Le téléphone détecte et affiche la vitesse de l'interface Ethernet en Mbit/s (c'est-à-dire 10 ou 100). Le message `Aucun Ethernet` signifie que la vitesse de l'interface du réseau LAN ne peut être déterminée. La vitesse Ethernet indiquée est la vitesse d'interface du réseau LAN du téléphone et de tout PC relié.
5. DHCP s'affiche pendant que le téléphone obtient une adresse IP ou autres informations du serveur DHCP du réseau LAN. Le nombre de secondes écoulées s'incrémente jusqu'à ce que l'interaction avec le serveur DHCP s'achève sans erreur.
  - Si le téléphone a été configuré à l'aide d'adresses statiques (en appuyant sur la touche \* lorsque DHCP s'affiche), il passe outre le serveur DHCP et utilise les paramètres d'adresse statique qui lui ont été donnés.
  - Remarquez que le chargement d'un nouveau fichier d'amorçage à tout moment efface toutes les informations sur les adresses statiques.
6. Une fois que le processus DHCP a pris fin sans rencontrer d'erreur, le téléphone demande des fichiers au serveur de fichiers défini dans la réponse DHCP. Le premier fichier répertorie les informations concernant les autres fichiers que le téléphone doit également charger. Le téléphone effectue d'abord sa demande de fichiers en utilisant le protocole HTTPS. En cas d'échec, il effectue la même demande en utilisant le protocole HTTP. Si cela échoue, il effectue une dernière demande en utilisant le protocole TFTP. Si toutes les requêtes de fichier échouent, le téléphone se remet à utiliser la version actuelle du fichier présent dans sa mémoire.
7. Une fois le script de mise à niveau téléchargé, la séquence dépend de l'état des fichiers actuellement conservés dans la mémoire des téléphones, par rapport à ceux qui sont énumérés dans le script de mise à niveau.

## Liens connexes

[Mise à jour nécessaire du fichier d'amorçage](#) à la page 119

[Aucun fichier d'application ou mise à jour nécessaire du fichier d'application](#) à la page 119  
[Fichier d'amorçage correct et fichier d'application déjà chargé](#) à la page 120

---

## Mise à jour nécessaire du fichier d'amorçage

Après avoir traité le fichier script de mise à jour, le logiciel détecte une différence entre le nom du fichier code d'amorçage du téléphone et celui inscrit dans le script de mise à jour. Le script précise le nom du nouveau fichier à charger.

1. Le téléphone affiche le nom du fichier et le nombre de kilo-octets chargés.
2. Le téléphone affiche le message `Saving to flash` pendant que le nouveau fichier d'amorçage est stocké dans sa mémoire flash. Le pourcentage de fichier stocké et le nombre de secondes écoulées sont indiqués. En général, cela ne dure pas plus de temps qu'il n'a fallu pour télécharger le fichier.
3. Le téléphone affiche le message `Redémarrage` lorsqu'il se prépare à redémarrer à l'aide du nouveau fichier d'amorçage.
4. Le téléphone affiche le message `Initialisation`.
5. Pendant que le nouveau fichier d'amorçage est décompressé dans la mémoire vive (RAM), le téléphone affiche le message `Chargement`. Comme ceci prend un certain temps, des astérisques, des points puis à nouveau des astérisques s'affichent sur la deuxième ligne pour indiquer une activité.
6. Lorsque le logiciel qui vient d'être chargé prend le contrôle, le téléphone affiche le message `Démarrage`.
7. Le téléphone affiche le message `Suppression` pendant que la mémoire flash est effacée afin de permettre la réécriture du code. Le pourcentage de mémoire effacée et le nombre de secondes écoulées sont indiqués.
8. Le message `Mise à jour` s'affiche tant que la réécriture du code d'amorçage est en cours. Le téléphone affiche également le pourcentage du code d'amorçage réécrit et le nombre de secondes qui se sont écoulées.
9. Quand le nouveau code d'amorçage a été écrit correctement dans la mémoire flash, le téléphone se réinitialise pour que l'état des fichiers d'application du téléphone puissent être vérifiés.

### Liens connexes

[Scénarios de redémarrage](#) à la page 118

---

## Aucun fichier d'application ou mise à jour nécessaire du fichier d'application

Cela se produit avec des mises à jour de fichiers d'application normaux. Après le traitement du fichier script de mise à jour, le logiciel détermine que le nom du fichier d'amorçage du

téléphone est la version correcte. Il détecte ensuite que le nom du fichier d'application ne correspond pas à celui stocké dans le téléphone.

1. Le téléphone affiche le nom du fichier nécessaire au moment du téléchargement du fichier à partir du serveur TFTP. Il affiche également le nombre de kilo-octets téléchargés.
2. Le message `Enregistrement sur la mémoire flash s'affiche`. Le téléphone affiche également le pourcentage stocké du fichier et le nombre de secondes écoulées. En général, cela ne dure pas plus de temps qu'il n'a fallu pour télécharger le fichier.
3. Le téléphone se réinitialise pour que le nouveau fichier d'application spécifique au système soit examiné.

#### Liens connexes

[Scénarios de redémarrage](#) à la page 118

---

## Fichier d'amorçage correct et fichier d'application déjà chargé

Ceci se produit avec la plupart des redémarrages normaux. Après le traitement du fichier script de mise à jour, le logiciel a vérifié que les noms du fichier d'amorçage du téléphone et du fichier d'application du téléphone correspondaient bien à ceux inscrits dans le script de mise à jour.

1. L'enregistrement spécifique au système auprès du commutateur démarre alors. Le téléphone demande le numéro de poste à utiliser et le mot de passe.
  - Par défaut, le téléphone affiche le dernier numéro de poste qu'il a utilisé. Pour accepter, appuyez sur #.
  - Lorsqu'une demande de mot de passe est indiquée, la vérification du mot de passe n'est pas effectuée si l'utilisateur change de numéro de poste.
  - La vérification du mot de passe s'effectue relativement au **Mot de passe du téléphone** stocké dans IP Office Manager. Si aucun **Mot de passe du téléphone** n'a pas été défini, le système effectue également une vérification en utilisant le code d'ouverture de session de l'utilisateur correspondant. Les systèmes IP Office antérieurs à la version 9.0 utilisent uniquement le **Code de connexion** de l'utilisateur correspondant.
2. Une fois l'enregistrement terminé, un signal retentit sur le téléphone si une licence de poste ou un abonnement utilisateur est disponible.

#### Liens connexes

[Scénarios de redémarrage](#) à la page 118

# Chapitre 20 : Ressources

---

## Documentation

---

### Recherche de documents sur le site Web du support technique d'Avaya

#### Procédure

1. Accédez à <https://support.avaya.com>.
2. En haut de l'écran, entrez votre nom d'utilisateur et votre mot de passe, puis sélectionnez **Login**.
3. Cliquez sur **Support by Product > Documents**.
4. Dans **Enter your Product Here**, entrez le nom du produit, puis sélectionnez-le dans la liste.
5. Dans **Choose Release**, sélectionnez la version appropriée.  
Le champ **Choose Release** n'est pas disponible s'il n'y a qu'une seule version du produit.
6. Dans le filtre **Content Type**, sélectionnez un type de document ou **Select All** pour afficher la liste de tous les documents disponibles.  
Par exemple, pour les guides d'utilisateur, sélectionnez **User Guides** au niveau du filtre **Content Type**. La liste affiche uniquement les documents correspondants à la catégorie sélectionnée.
7. Cliquez sur **Enter**.

---

## Formation

---

### Visualiser les vidéos Avaya Mentor

Les vidéos de Avaya Mentor expliquent comment installer et configurer les produits Avaya et comment résoudre les problèmes rencontrés.

## À propos de cette tâche

Ces vidéos sont disponibles sur le site du support technique Avaya, répertoriées dans la catégorie correspondante et sur la chaîne YouTube Avaya.

- Pour trouver des vidéos sur le site web de l'Assistance technique d'Avaya, rendez-vous sur <https://support.avaya.com/> et effectuez l'une des manipulations suivantes :
  - Dans **Search**, saisissez *Avaya Mentor Videos*, cliquez sur **Clear All** et sélectionnez **Video** dans le champ **Content Type**.
  - Dans **Search**, saisissez le nom du produit. Sur la page **Search Results**, cliquez sur **Clear All** et sélectionnez **Video** dans le champ **Content Type**.

Le type de contenu **Video** ne s'affiche que si des vidéos concernant ce produit sont disponibles.

Dans le volet de droite, la page affiche une liste des vidéos disponibles.

- Pour accéder aux vidéos de Avaya Mentor sur YouTube, accédez à [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor), et effectuez l'une des manipulations suivantes :
  - Saisissez un ou plusieurs mots-clés dans le champ **Search Channel** pour rechercher un produit ou un sujet spécifique.
  - Faites défiler les **Playlists**, puis cliquez sur le nom d'un sujet pour afficher la liste des vidéos associées qui sont disponibles. Par exemple, Contact Centers.

### \* Remarque :

Les vidéos ne sont pas disponibles pour tous les produits.

---

## Support technique

Visitez le site Web de l'assistance technique d'Avaya à l'adresse <https://support.avaya.com> pour obtenir la documentation, les notices de produits et les articles de connaissance les plus récents. Vous pouvez également rechercher des notes de mise à jour, des téléchargements et des résolutions aux problèmes rencontrés. Utilisez le système de demande de service en ligne pour créer une demande de service. Discutez avec des agents en temps réel pour obtenir des réponses à vos questions ou pour demander d'être mis en relation avec une équipe du support technique dans le cas où un problème nécessiterait une expertise supplémentaire.

### Liens connexes

[Utilisation de l'InSite Knowledge Base \(base de connaissances sur site\) d'Avaya](#) à la page 122

---

## Utilisation de l'InSite Knowledge Base (base de connaissances sur site) d'Avaya

La base de connaissances sur site d'Avaya est un moteur de recherche basé sur le Web qui fournit ce qui suit :

- Des astuces techniques et des procédures de détection de pannes actualisées
- Les informations relatives aux service packs

- L'accès à la documentation technique et à celle destinée aux clients
- Les informations relatives aux programmes de formation et de certification
- Les liens vers d'autres informations pertinentes

Vous pouvez avoir accès à la base de connaissances sans frais supplémentaires si vous êtes un partenaire reconnu ou un client actuel d'Avaya possédant un contrat d'assistance technique. Vous devez posséder un compte et un numéro Sold-To (vendu à) valides.

Utilisez l'InSite Knowledge Base (base de connaissances sur site) d'Avaya pour rechercher d'éventuelles solutions à vos problèmes.

1. Accédez à <http://www.avaya.com/support>.
2. Connectez-vous au site Web d'Avaya à l'aide d'un mot de passe et d'un ID utilisateur Avaya valides.

Le système affiche la page **Avaya Support**.

3. Cliquez sur **Support by Product > Product-specific Support**.
4. Dans **Enter Product Name**, saisissez le nom du produit, puis appuyez sur la touche **Entrée**.
5. Dans la liste, sélectionnez le produit, puis la version souhaitée.
6. Cliquez sur l'onglet **Technical Solutions** pour afficher les articles.
7. Sélectionnez les articles qui vous intéressent.

#### Liens connexes

[Support technique](#) à la page 122

# Index

<a href="#">_activer</a>	
<a href="#">protocole SRTP au niveau du système</a>	<a href="#">98</a>
<a href="#">46xxspecials.txt</a>	<a href="#">31</a>
<b>A</b>	
<a href="#">activation</a>	
<a href="#">champ d'application</a>	<a href="#">97</a>
<a href="#">interface du concentrateur</a>	<a href="#">109, 110</a>
<a href="#">protocole SRTP au niveau du système</a>	<a href="#">99</a>
<a href="#">rapports de qualité du système</a>	<a href="#">64</a>
<a href="#">rapports de qualité sur les téléphones</a>	<a href="#">63</a>
<a href="#">responsable de passerelle H.323</a>	<a href="#">39</a>
<a href="#">série 9600</a>	<a href="#">110</a>
<a href="#">surveillance de la qualité du protocole RTCP</a>	<a href="#">63</a>
<a href="#">TLS sur le système IPO</a>	<a href="#">104</a>
<a href="#">TLS sur les téléphones</a>	<a href="#">104</a>
<a href="#">Administrateur</a>	
<a href="#">Statique</a>	<a href="#">107</a>
<a href="#">Administration statique</a>	<a href="#">107</a>
<a href="#">adresse statique</a>	
<a href="#">installation</a>	<a href="#">75</a>
<a href="#">paramètres</a>	<a href="#">76, 77</a>
<a href="#">affichage des détails</a>	
<a href="#">téléphones de la série 9600</a>	<a href="#">112</a>
<a href="#">afficher les détails</a>	
<a href="#">téléphones</a>	<a href="#">111</a>
<a href="#">téléphones de la série 1600</a>	<a href="#">111</a>
<a href="#">ajout</a>	
<a href="#">certificat d'identité</a>	<a href="#">102</a>
<a href="#">option 242</a>	<a href="#">96</a>
<a href="#">alimentation</a>	
<a href="#">alimentation</a>	<a href="#">23</a>
<a href="#">options</a>	<a href="#">23</a>
<a href="#">autres</a>	
<a href="#">options</a>	<a href="#">92</a>
<b>B</b>	
<a href="#">blocage</a>	
<a href="#">codes d'accès par défaut</a>	<a href="#">28</a>
<b>C</b>	
<a href="#">canaux</a>	<a href="#">19</a>
<a href="#">champ d'application</a>	<a href="#">95</a>
<a href="#">chargement</a>	
<a href="#">certificat</a>	<a href="#">103</a>
<a href="#">fichiers</a>	<a href="#">53</a>
<a href="#">fichiers du logiciel</a>	<a href="#">50</a>
<a href="#">chargement de fichiers</a>	
<a href="#">serveur tiers</a>	<a href="#">53</a>
<a href="#">configuration</a>	
<a href="#">fichier</a>	<a href="#">33</a>
<a href="#">configuration (suite)</a>	
<a href="#">plage de ports RTP</a>	<a href="#">39</a>
<a href="#">serveur Apache</a>	<a href="#">72</a>
<a href="#">serveur IIS</a>	<a href="#">72</a>
<a href="#">seuils d'alarme de qualité</a>	<a href="#">65</a>
<a href="#">Système IPO</a>	<a href="#">81</a>
<a href="#">téléphone IP</a>	<a href="#">85</a>
<a href="#">VPN distant</a>	<a href="#">85</a>
<a href="#">connexion</a>	
<a href="#">téléphone</a>	<a href="#">59</a>
<a href="#">contrôle</a>	
<a href="#">cartes mémoire d'unité</a>	<a href="#">26</a>
<a href="#">création</a>	
<a href="#">fichier de paramètres</a>	<a href="#">48</a>
<b>D</b>	
<a href="#">définition</a>	
<a href="#">valeur BRURI</a>	<a href="#">69</a>
<a href="#">désactivation</a>	
<a href="#">SRTP</a>	<a href="#">99</a>
<a href="#">téléphone</a>	<a href="#">115</a>
<a href="#">téléphones de la série 1600</a>	<a href="#">116</a>
<a href="#">téléphones de la série 9600</a>	<a href="#">116</a>
<a href="#">désactivation sur</a>	
<a href="#">ligne</a>	<a href="#">99</a>
<a href="#">poste</a>	<a href="#">99</a>
<a href="#">DHCP</a>	
<a href="#">Autre configuration du serveur</a>	<a href="#">92</a>
<a href="#">paramètres</a>	<a href="#">43</a>
<a href="#">distant</a>	<a href="#">79</a>
<b>E</b>	
<a href="#">économiseur d'écran</a>	<a href="#">66</a>
<a href="#">paramètres</a>	<a href="#">67</a>
<a href="#">enregistrement</a>	
<a href="#">téléphone</a>	<a href="#">60</a>
<a href="#">enregistrements</a>	
<a href="#">mise sur liste noire</a>	<a href="#">28</a>
<a href="#">exemple</a>	
<a href="#">fichier</a>	<a href="#">70</a>
<a href="#">exemple de configuration</a>	
<a href="#">présentation</a>	<a href="#">87</a>
<a href="#">exemple de système</a>	
<a href="#">présentation</a>	<a href="#">90</a>
<b>F</b>	
<a href="#">fichier</a>	
<a href="#">génération automatique</a>	<a href="#">27</a>
<a href="#">serveur</a>	<a href="#">24</a>
<a href="#">Fichier</a>	
<a href="#">paramètres du serveur</a>	<a href="#">46</a>
<a href="#">fichier d'amorçage correct</a>	
<a href="#">fichier d'application</a>	<a href="#">120</a>
<a href="#">fichier d'application</a>	

fichier d'application ( <i>suite</i> )		par défaut ( <i>suite</i> )	
mise à jour .....	<a href="#">119</a>	mot de passe du poste .....	<a href="#">54</a>
fichier de démarrage		paramétrage	
mise à jour .....	<a href="#">119</a>	de la qualité de service (QoS) de DiffServ .....	<a href="#">41</a>
<b>G</b>		paramètres	
génération automatique .....	<a href="#">14</a>	économiseur d'écran .....	<a href="#">67</a>
<b>H</b>		paramètres du serveur de fichiers .....	<a href="#">48</a>
HTTP		pc	
authentification .....	<a href="#">69</a>	connexion .....	<a href="#">23</a>
<b>I</b>		personnalisation	
InSite Knowledge Base (base de connaissances sur		fonctionnement .....	<a href="#">67</a>
site) .....	<a href="#">122</a>	potentiels	
IP500		VoIP .....	<a href="#">22</a>
unité de contrôle .....	<a href="#">51</a>	pris en charge	
<b>L</b>		Téléphone VPN distant .....	<a href="#">84</a>
Licence		Téléphones IP .....	<a href="#">11</a>
abonnements .....	<a href="#">18, 37</a>	problèmes .....	<a href="#">22</a>
liste		procédure de test automatique	
téléphones enregistrés .....	<a href="#">61</a>	téléphones de la série 1600 .....	<a href="#">113</a>
<b>M</b>		téléphones de la série 9600 .....	<a href="#">114</a>
manuel		processus administrateur	
sauvegarde .....	<a href="#">70</a>	mot de passe .....	<a href="#">109</a>
manuelle		<b>Q</b>	
copier de fichiers .....	<a href="#">52</a>	QoS .....	<a href="#">21</a>
création de postes .....	<a href="#">56</a>	<b>R</b>	
modification d'un fichier .....	<a href="#">50</a>	redémarrage .....	<a href="#">118</a>
modification		réinitialisation	
fichier .....	<a href="#">33</a>	téléphone .....	<a href="#">114</a>
fichier de paramètres .....	<a href="#">48</a>	téléphone de la série 1600 .....	<a href="#">114</a>
paramètres du serveur de fichiers .....	<a href="#">47</a>	téléphone de la série 9600 .....	<a href="#">115</a>
paramètres SSON du système .....	<a href="#">44</a>	réseau	
modifier		évaluation .....	<a href="#">18</a>
mot de passe craft .....	<a href="#">102</a>	réseau client	
<b>N</b>		configuration .....	<a href="#">80</a>
nouser		réservation	
source .....	<a href="#">32</a>	licences .....	<a href="#">37</a>
nouveau		restauration	
version .....	<a href="#">11</a>	contrôle .....	<a href="#">70</a>
<b>O</b>		paramètres .....	<a href="#">68</a>
options administratives		<b>S</b>	
série 1600 .....	<a href="#">108</a>	saisie	
série 9600 .....	<a href="#">108</a>	options administratives .....	<a href="#">108</a>
<b>P</b>		sauvegarde	
par défaut		paramètres .....	<a href="#">68</a>
		sélection	
		codec .....	<a href="#">56</a>
		serveur	
		options .....	<a href="#">24</a>
		simple	
		installation .....	<a href="#">14</a>
		site du système	
		numéros d'option spécifiques .....	<a href="#">44</a>
		Site Web d'assistance Avaya .....	<a href="#">122</a>
		source	
		numbers .....	<a href="#">32</a>

## Index

spécifique au site	
numéro d'option .....	<a href="#">116</a>
SRTP .....	<a href="#">98</a>
SSON	
téléphones de la série 1600 .....	<a href="#">117</a>
téléphones de la série 9600 .....	<a href="#">117</a>
supplémentaires du téléphone	
paramètres .....	<a href="#">30</a>
support direct .....	<a href="#">100</a>
support technique .....	<a href="#">122</a>
système	
capacité .....	<a href="#">12</a>
codecs par défaut .....	<a href="#">41</a>
prise en charge DHCP .....	<a href="#">43</a>

## T

téléchargement	
certificat d'identité .....	<a href="#">103</a>
téléchargement à partir de	
serveur basé sur Linux .....	<a href="#">103</a>
téléphone	
configuration .....	<a href="#">82</a>
demandes de fichiers .....	<a href="#">26</a>
micrologiciel .....	<a href="#">13</a>
TLS .....	<a href="#">101</a>

## U

unité de contrôle	
carte mémoire .....	<a href="#">28</a>
utilisateur	
création des postes .....	<a href="#">54</a>
pc .....	<a href="#">23</a>
utilisation	
création automatique .....	<a href="#">57</a>
options d'administration statique .....	<a href="#">107</a>
utilisation du gestionnaire de fichiers intégré	
charger des fichiers .....	<a href="#">51</a>

## V

vérification	
fonctionnement TLS .....	<a href="#">105</a>
prise en charge du serveur DHCP .....	<a href="#">94</a>
vidéos .....	<a href="#">121</a>
VLAN	
DHCP .....	<a href="#">86</a>
Téléphones IP .....	<a href="#">85</a>
voix	
compression .....	<a href="#">19</a>
VPN	
téléphones à distance .....	<a href="#">83</a>