IP Office™ Platform 12.0

Guide d'administration d'Avaya one-X Portal for IP Office

15-601139 Version 19a - (15/04/2024)

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 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.

Clause de non-responsabilité en matière de documentation
Le terme « Documentation »désigne toute information publiée sur différents supports, pouvant inclure des informations sur les produits, des descriptions d'abonnements ou de services, des instructions sur le fonctionnement et des spécifications de performance généralement mises à la disposition des utilisateurs de ces produits. Le terme Documentation n'inclut pas les supports 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 ceux-ci sont effectués par l'utilisateur final.

Clause de non-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 la Documentation fourniepar 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 qui y sont associées.

Garantie
Avaya offre une garantie limitée sur le matériel et les logiciels Avaya. Veuillez vous référer à votre contrat avec Avaya pour en connaître les termes. Les clients d'Avaya trouveront 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 l'assistance technique Avaya à l'adresse suivante : https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 sous la rubrique « Garantie etcycle de vie du produit », 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 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 « UTILISATEURFINAL »), 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 générales de licence de logiciel (les « Conditions delicence de logiciel ») sont disponibles sur le site Web suivant : https://w w w .avaya.com/en/legal-license-terms/, ou sur tout site successeur désigné par Avaya. Les présentes Conditions de licence de logiciel s'appliquent à toute personne qui installe, télécharge et/ou utilise le Logiciel et/ou la Documentation. En installant, en téléchargeant ou en utilisant le Logiciel, ou en autorisant d'autres personnes à le faire, l'utilisateur final accepte que les présentes Conditions de licence de logiciel le lient par contrat à Avaya. Si l'utilisateur final accepte les présentes Conditions de licence de logiciel au nom d'une société ou d'une autre entité juridique, l'utilisateur final déclare avoir le pouvoir de lier ladite entité aux présentes Conditions de licence de logiciel.

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 licences 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, charger, 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 ou l'utilisation non autorisés de ce contenu 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
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).

Fournisseur de service
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).

Dans le respect des lois
Vous reconnaissez et acceptez être tenu responsable de vous conformer aux lois et règlements applicables, y compris, mais 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 que vous avez besoin d'une assistance technique ou autre, veuillez contacter votre représentant commercial Avaya.

Failles 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 commerciales
Les marques commerciales, les logos et les marques de service (« Marques ») figurant sur ce site, sur toute documentation, sur 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 LLC.
Toutes les marques commerciales autres qu'Avaya sont la propriété de leurs détenteurs respectifs.
Linux® est une marque de commerce déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

Téléchargement de la documentation
Pour obtenir les versions les plus récentes de la Documentation, reportez-vous au site Web de l'assistance technique Avaya : https://support.avaya.com, ou au site successeur désigné par Avaya.

Contacter l'assistance Avaya
Consultez le site Web de l'assistance technique Avaya : https://support.avaya.com pour obtenir des avis et des articles portant sur les produits ou les services cloud, ou pour signaler tout problème que vous pourriez rencontrer avec votre produit ou service cloud Avaya. Pour connaître nos coordonnées et obtenir la liste des numéros d'assistance, consultez le site Web de l'assistance technique Avaya à l'adresse : https://support.avaya.com (ou le site successeur désigné par Avaya), faites défiler la page jusqu'en bas, puis sélectionnez Contacter l'assistance Avaya.

Table des matières

1. one-X Portal for IP Office Administration

1.1 Se connecter 9
1.2 Se déconnecter 9

2. Menus d'administration

2.1 État d'intégrité 14
2.1.1 Tableau de bord 14
2.1.2 État des composants 15
2.1.3 État du serveur MI/Présence 15
2.1.4 Résilience 16
2.1.5 Événements récents majeurs 17
2.1.6 Sessions actives 18
2.1.7 Environnement 18
2.2 Configuration 19
2.2.1 Fournisseurs 19
2.2.2 Utilisateurs 24
2.2.3 CSV 25
2.2.4 Personnalisation 25
2.2.5 MI/Présence 26
2.2.6 Service Exchange 27
2.2.7 Configuration SMTP 28
2.2.8 Accès distant à une conférence 29
2.2.9 Résilience 30
2.2.10 Nom de domaine de l'hôte 32
2.2.11 Nettoyage de conférence 32
2.2.12 Lien CTI central 33
2.2.13 Bloquer les versions du client 34
2.3 Sécurité 34
2.3.1 Protocole HTTP/HTTPS 34
2.3.2 Paramètres TLS 35
2.3.3 Authentification ESNA 35
2.3.4 Certificat 35
2.4 Diagnostics 36
2.4.1 Configuration des journaux 36
2.4.2 Visionneuse de journaux 38
2.4.3 Itinéraires réseau 38
2.4.4 Connexions IP Office 39
2.4.5 Intégrité de la base de données 39
2.4.6 Validation des données utilisateur 40
2.4.7 Programmation d'appel/de conférence 41
2.4.8 Affichage des conférences 42
2.4.9 Générer un fichier de vidage mémoire 43
2.4.10 Générer un thread dump 43
2.5 Intégration des répertoires 43
2.5.1 Synchronisation des répertoires 43
2.5.2 Recherche dans le répertoire LDAP 43
2.5.3 Annuaire système 45
2.6 Configuration des gadgets 46
2.6.1 Liste des gadgets externes 46
2.6.2 Importation de gadgets 46
2.6.3 Exportation de gadgets 47
2.7 Archives MI 48
2.7.1 Rechercher dans les archives 48
2.8 Conférences Web 49
2.8.1 Contrôler les conférences 49
2.9 Aide et assistance technique 50

3. Tâches de maintenance

3.1 Redémarrage du service 52
3.2 Configuration du journal des appels 53
3.3 Commutateur IP Office 54
3.3.1 Ajout d'un système IP Office supplémentaire 54
3.3.2 Modification des détails IP Office 56
3.3.3 Résilience 57
3.4 Gadgets 60
3.4.1 Récupération de l'URL d'un gadget 60
3.4.2 Importation de gadgets 61
3.4.3 Exportation de gadgets 63
3.4.4 Ajout d'un gadget externe 64
3.4.5 Modification d'un gadget externe 64
3.4.6 Activation d'un gadget externe 65
3.4.7 Désactivation d'un gadget externe 65
3.4.8 Suppression d'un gadget externe 65
3.5 Utilisateurs 66
3.5.1 Ajout/Suppression d'utilisateurs 66
3.5.2 Modification des paramètres utilisateur 66
3.6 Annuaires 68
3.6.1 Ajout d'une source de répertoire LDAP externe 68
3.6.2 Vérification du répertoire LDAP externe 70
3.6.3 Vérification et mise à jour du répertoire système 71
3.7 Mise à niveau supérieure/Mise à niveau inférieure 72
3.7.1 Mise à niveau de one-X Portal for IP Office 72
3.7.2 Rétrogradation de one-X Portal for IP Office 73
3.7.3 Suppression de one-X Portal for IP Office 74
3.8 Messagerie instantanée/Présence 76
3.8.1 Configuration du serveur MI 77
3.8.2 Configuration MI utilisateur 79
3.8.3 Démarrage du serveur MI 79
3.8.4 Recherche dans les archives MI 80
3.8.5 Intégration du calendrier Exchange 81
3.8.6 Activation de la console d'administration XMPP 82
3.8.7 Activation des archives MI 82
3.8.8 Désactivation des archives MI 83
3.8.9 Désactivation de la console d'administration XMPP 83
3.9 Conférences 84
3.9.1 Affichage des conférences 84
3.9.2 Affichage des conférences planifiées 85
3.9.3 Suppression d'une conférence programmée 86
3.9.4 Message de notification de conférence 86
3.9.5 E-mails de conférence 87
3.9.6 Définition de l'URL de collaboration Web 88
3.10 Consultation des journaux à distance 89
3.11 Dépannage 93
3.12 Ajouter des administrateurs supplémentaires 94

4. Menus AFA

4.1 Se connecter 96
4.2 État du système 97
4.3 Configuration 97
4.4 Fonctionnements DB 98

4.4.1 Sauvegarde 98
4.4.2 Restauration 99
Index 101

Chapitre 1.

one-X Portal for IP Office Administration

1. one-X Portal for IP Office Administration

En plus de permettre un fonctionnement normal pour l'utilisateur final, l'interface Web one-X Portal for IP Office offre également plusieurs fonctions d'administration et de maintenance. Cette documentation est notamment consacrée à l'utilisation de ces menus d'administration.

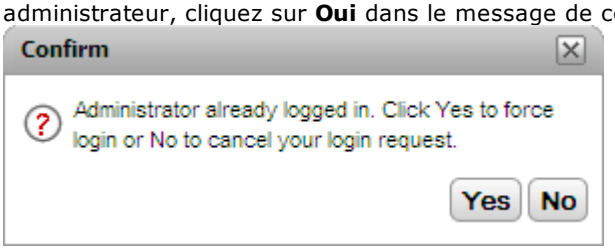
1.1 Se connecter

A l'instar de l'accès des utilisateurs, l'accès aux menus d'administration de one-X Portal for IP Office se fait via un navigateur Web, en ajoutant toutefois ***?admin=true*** à l'URL. Un seul utilisateur à la fois peut se connecter en tant qu'administrateur.

- Par défaut les serveurs one-X Portal for IP Office sous Linux utilisent l'**authentification référée**. Cela signifie que les droits d'administration du portail sont attribués aux utilisateurs de sécurité configurés dans la configuration de sécurité du service IP Office exécuté sur le même serveur. Il s'agit par défaut de l'utilisateur **Administrateur**, mais il est possible de configurer des utilisateurs de service supplémentaires qui pourront accéder à l'administration du portail.
- Si l'authentification référée est désactivée, le portail utilise son propre compte d'administration local de la même manière que sur un serveur Windows, tel que décrit ci-dessous.

Pour vous connecter :

1. Dans le navigateur web, saisissez l'URL sous la forme suivante : ***https://<nom du serveur>:<port du serveur>/onexportal-admin.html***, où :
   - ***<nom du serveur>*** est le nom ou l'adresse IP du serveur one-X Portal for IP Office.
   - ***<port du serveur>*** est le numéro de port utilisé par one-X Portal for IP Office. Il peut s'agir du port 9443 ou du port 8443 pour l'accès HTTPS.
   - Vous pouvez utiliser ***http://*** plutôt que ***https://*** et ***8080*** comme port si un accès non sécurisé a été configuré. Voir Protocole 34.
   - Autre possibilité : dans le menu de connexion utilisateur normal, sélectionnez **Connexion administrateur**.
2. Saisissez le nom et le mot de passe administrateur de one-X Portal for IP Office configurés au cours de l'installation.
   - Si une session d'administrateur est déjà ouverte, le message de confirmation suivant s'affiche : Pour fermer la session d'administrateur ouverte et vous connecter avec vos propres accréditations administrateur, cliquez sur **Oui** dans le message de confirmation.

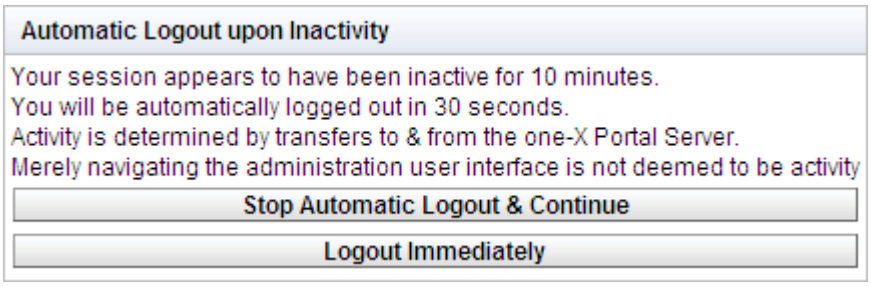


3. Cliquez sur **Connexion**.

1.2 Se déconnecter

L'option **Déconnexion** en haut à droite des menus d'administration one-X Portal for IP Office permet de se déconnecter.

Parallèlement à la déconnexion manuelle, vous serez aussi invité à vous déconnecter après 10 minutes. Si vous ne répondez pas, vous serez automatiquement déconnecté.



Chapitre 2.
Menus d'administration

2. Menus d'administration

Le menu d'administration de one-X Portal for IP Office propose un éventail d'options pour la surveillance et la configuration de l'application one-X Portal for IP Office.

Menu	Sous-menu	Description
État d'intégrité	**Tableau de bord** 14	Affiche un résumé de l'état du serveur.
	État des composants 15	Dresse la liste du dernier changement d'état des composants du serveur.
	État du serveur MI/Présence 15	Affiche l'état actuel du composant du serveur de messagerie instantanée.
	Résilience 16	Affiche l'état des serveurs en configuration résiliente. *(IP Office Server Edition uniquement)*
	Événements récents majeurs 17	Permet d'afficher les 20 derniers événements qui se sont produits sur le serveur.
	Sessions actives 18	Indique le nombre de sessions mises en cache par one-X Portal for IP Office.
	Environnement 18	Permet d'afficher le récapitulatif du PC du serveur one-X Portal for IP Office.
Configuration	**Fournisseurs** 19	Permet d'afficher et de modifier les fournisseurs.
	Utilisateurs 24	Permet d'afficher et de modifier les paramètres des utilisateurs de one-X Portal for IP Office.
	CSV 25	Permet d'exporter le répertoire des utilisateurs et le répertoire système.
	Personnalisation 25	Permet de définir le texte apparaissant sur les pages one-X Portal for IP Office lorsqu'un utilisateur est connecté.
	MI/Présence 26	Permet de contrôler l'état du serveur MI/Présence en tant qu'Administrateur.
	Service Exchange 27	Permet de configurer le serveur Exchange pour exploiter l'exploration de calendrier et les informations de présence des utilisateurs.
	Configuration SMTP 28	Permet de définir les informations relatives au courrier électronique employé pour l'envoi des notifications des conférences.
	Accès distant à une conférence 29	Permet de saisir le texte fixe à inclure dans les notifications des conférences programmées.
	Résilience 30	Utilisée sur un IP Office Application Server pour définir si un portail assure une prise en charge de la résilience. *(IP Office Server Edition Select uniquement)*
	Nom de domaine de l'hôte 32	Permet de définir l'URL utilisée dans les invitations à une conférence de collaboration Web.
	Nettoyage de conférence 32	Configurez le délai pendant lequel les informations des conférences sont conservées.
	Lien CTI central 33	Permet de configurer si le serveur détecte et prend en charge automatiquement les autres systèmes IP Office d'un réseau.
	Bloquer les versions du client 34	Configurez des versions et des builds de clients spécifiques que le serveur ne prend pas en charge.
Sécurité	**Protocole HTTP/HTTPS** 34	Permet de définir si le serveur doit utiliser HTTPS ou HTTPS et HTTP.
	Paramètres TLS 35	Permet de configurer les options de prise en charge TLS.
	Authentification ESNA 35	Permet de définir l'adresse du serveur ESNA utilisé pour authentifier les utilisateurs se connectant par le biais d'un compte ESNA.
Diagnostics	**Configuration des journaux** 36	Permet de configurer le niveau et le mode de consignation pris en charge.
	Visionneuse de journaux 38	Permet d'installer et de lancer Chainsaw pour consulter les journaux.
	Itinéraires réseau 38	Permet de tester le chemin de connexion IP vers une adresse IP.

Menu	Sous-menu	Description
	Connexions IP Office 39	Permet de tester le chemin de connexion IP vers un système IP Office.
	Intégrité de la base de données 39	Permet de tester la structure de la base de données.
	Validation des données utilisateur 40	Permet d'identifier les raisons pouvant expliquer l'échec de connexion d'un utilisateur ou la corruption de données utilisatur et de réinitialiser les données corrompues.
	Programmation d'appel/de conférence 41	Permet de supprimer une conférence programmée.
	Affichage des conférences 42	Affiche les détails des conférences planifiées historiques et futures pour tous les utilisateurs. Permet également de modifier et de supprimer ces conférences.
	Générer un fichier de vidage mémoire 43	Créez un rapport d'analyse relatif à l'utilisation actuelle de la mémoire du serveur.
	Générer un thread dump 43	Créez un rapport d'analyse relatif aux threads actuels du processeur.
Intégration des répertoires	Synchronisation des répertoires 43	Permet de forcer le serveur à mettre à jour le répertoire système.
	Annuaire système 45	Permet d'afficher le répertoire système de one-X Portal for IP Office.
	Recherche dans le répertoire LDAP 43	Permet d'afficher le répertoire externe pour lequel le serveur one-X Portal for IP Office a été configuré.
Configuration des gadgets	Liste des gadgets externes 46	Les gadgets externes présents dans le système sont répertoriés.
	Importer les gadgets externes 61	Permet d'importer les gadgets externes.
	Exporter les gadgets externes 47	Permet d'exporter les gadgets externes.
Conférences Web	Contrôler les conférences 49	Permet de consulter les informations de toute conférence Web actuellement en cours sur le serveur.
Archives MI	Rechercher dans les archives 48	Permet de rechercher des conversations par MI entre plusieurs contacts enregistrés dans le système.
Aide et assistance technique	Aide 50	Permet d'accéder à l'aide de one-X Portal for IP Office qui est installée sur le serveur.
	Assistance technique Avaya 50	Permet d'accéder au site Web de l'assistance technique d'Avaya pour les applications Avaya.
	À propos de 50	Permet d'afficher des informations sur la version de one-X Portal for IP Office.

Il est important de bien comprendre que les menus d'administration de one-X Portal for IP Office fonctionnent sous forme d'un éditeur hors ligne. Dans un menu particulier, les données sont récupérées de la base de données (à l'aide d'une commande **GET**), modifiées, puis renvoyées à la base de données (à l'aide d'une commande **PUT**).

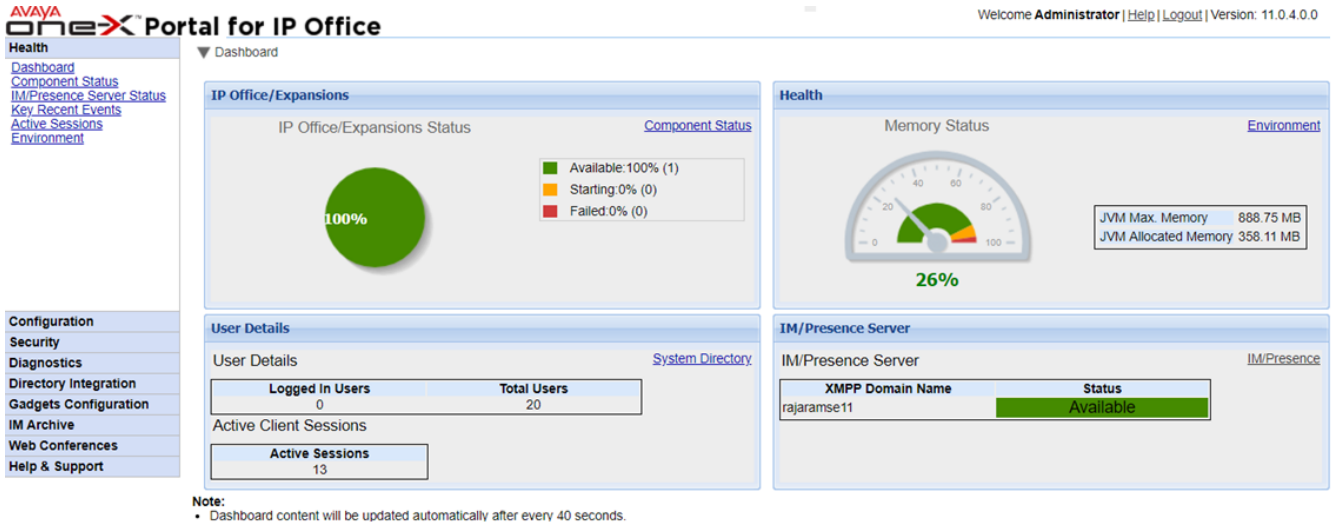
Dans tous les menus, vous pouvez cliquer sur les icônes ▶ ▼ pour afficher/masquer une brève description du rôle et du contenu des menus.

2.1 État d'intégrité

Cette section vous permet d'afficher l'état des différents composants du serveur.

2.1.1 Tableau de bord

Le menu Tableau de bord fournit un résumé de l'état du serveur.

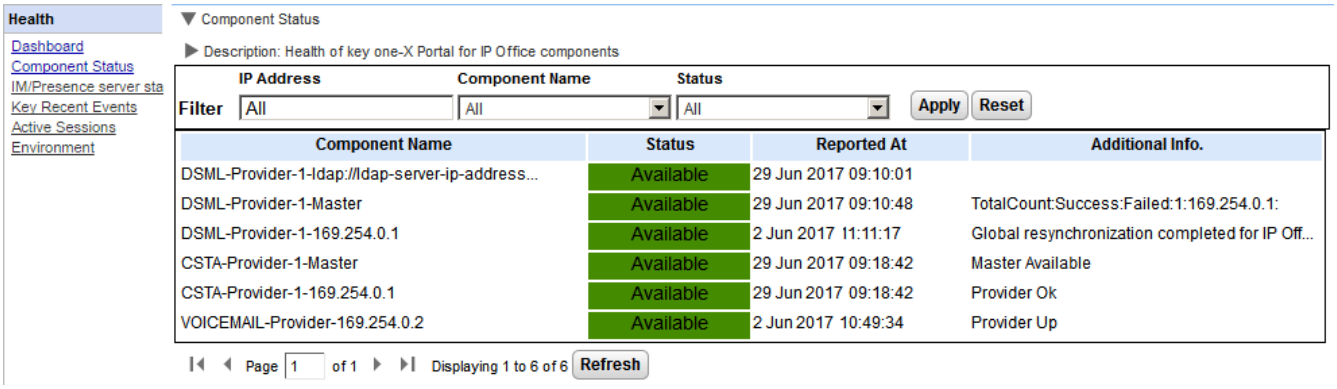


- **IP Office/État d'expansion**
  Cette section résume l'état des connexions entre le serveur de portail et les systèmes IP Office qu'il prend en charge.
- **Santé**
  Cette section donne un résumé de l'utilisation de la mémoire des serveurs.
- **Informations utilisateur**
  Cette section indique le nombre d'utilisateurs configurés et connectés. Elle indique également le nombre de sessions actives qui inclut les utilisateurs d'Avaya Communicator for Web, du plug-in Outlook et de one-X Portal for IP Office.
- **Serveur MI/Présence**
  Cette section résume l'état du composant XMPP du serveur.

2.1.2 État des composants

Le menu **État des composants** affiche les dernières modifications de l'état enregistré de chaque composant principal de l'application one-X Portal for IP Office.

- Pour les serveurs UCM, chaque système IP Office pris en charge doit être associé à un fournisseur CSTA principal de même qu'à un second fournisseur CSTA. Cette règle s'applique également aux systèmes Linux prenant en charge un réseau IP Office Server Edition mais n'utilisant pas le mode lien CTI centralisé 33.
- Pour un service dans un réseau IP Office Server Edition qui utilise le mode de lien CTI centralisé, il ne doit y avoir qu'un seul fournisseur DMSL pour le système IP Office principal. Il doit également y avoir un fournisseur CSTA pour le système IP Office principal, sauf si vous utilisez la résilience de portail, auquel cas il doit également y avoir un fournisseur CSTA pour le système IP Office secondaire.
- De plus, si vous utilisez LDAP, il doit également y avoir un fournisseur DSML LDAP.

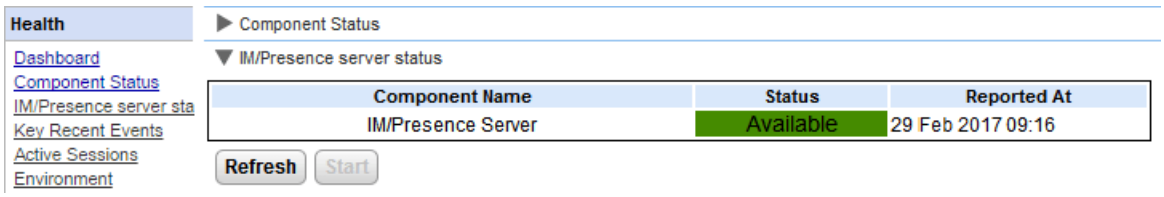


Pour afficher l'état du composant :

1. Sélectionnez **Santé**, puis **État des composants**.
2. Cliquez sur **Obtenir tout** pour récupérer les enregistrements d'état figurant dans la base de données de one-X Portal for IP Office.
3. Utilisez les commandes de la page pour faire défiler les enregistrements.
4. L'option **Supprimer** supprime l'enregistrement d'état, sans affecter le composant. Les cases à cocher et l'option **Supprimer les sélections** peuvent servir à effacer plusieurs enregistrements.

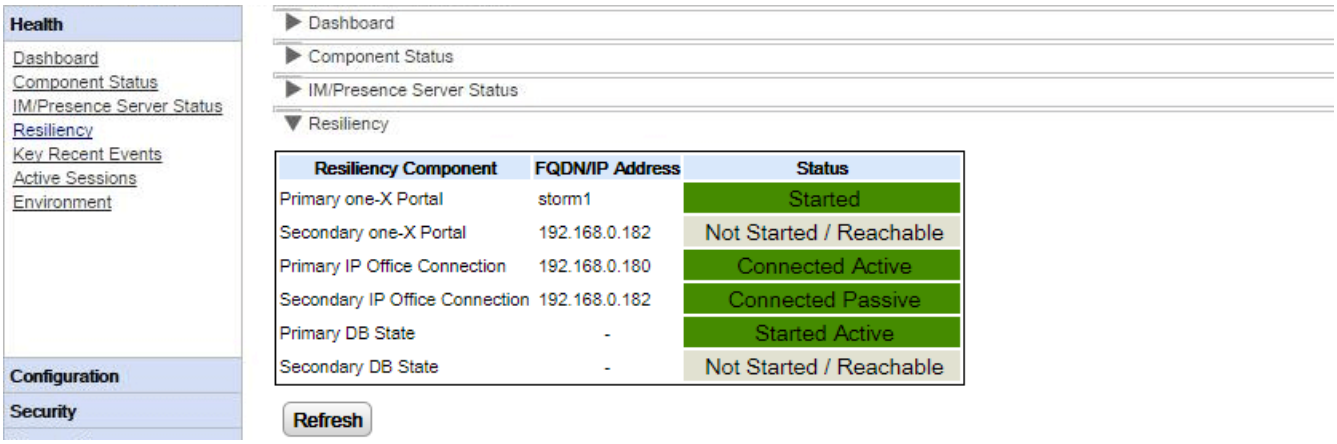
2.1.3 État du serveur MI/Présence

Ce menu affiche l'état actuel du serveur de messagerie instantanée utilisé comme service composant par le one-X Portal for IP Office. Pour plus d'informations sur plusieurs procédures de maintenance liées à la MI et à la présence, voir Messagerie instantanée 76.



2.1.4 Résilience

Ce menu apparaît sur les serveurs de portail du réseau IP Office Server Edition Select. Il indique l'état actuel du portail et des services IP Office sur les serveurs principal et secondaire lors de l'utilisation de la résilience IP Office Server Edition 16.



Par exemple, la capture d'écran ci-dessus montre un système dans lequel les serveurs principal et secondaire IP Office, ainsi que le serveur de portail principal fonctionnent, mais dans lequel le service de portail secondaire n'a pas été démarré. Lorsque le service de portail a démarré, l'état du portail secondaire devient ***Démarré*** et celui du **DB secondaire** devient ***Démarré passif***.

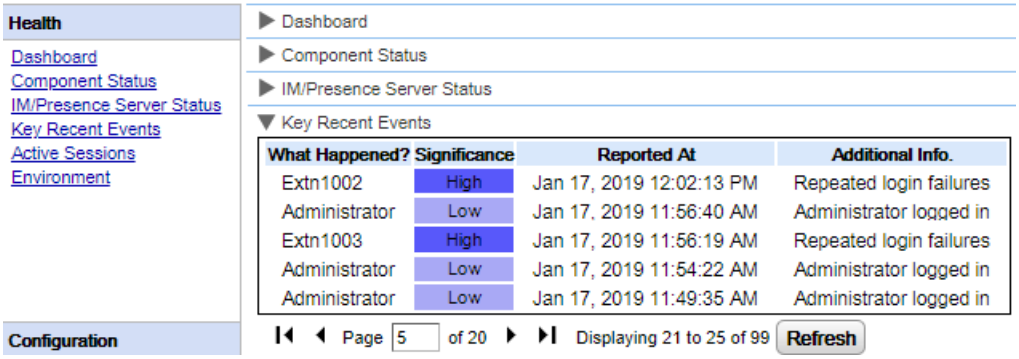
Les termes utilisés sur l'affichage d'état ont les significations suivantes. Les termes peuvent être associés :

- **Démarré**
  Le service est en cours d'exécution.
- **Arrêté** ou **Non démarré**
  Le service n'est pas en cours d'exécution.
- **Connecté**
  Ce serveur de portail possède une connexion au service.
- **Accessible**
  Le service qui héberge le service a été détecté, mais il n'y a aucune connexion car le service sur ce serveur n'a pas été démarré.
- **Actif**
  Le service est actuellement utilisé pour assurer la prise en charge des utilisateurs du portail.
- **Passif**
  Le service est en cours d'exécution, mais n'est actuellement pas utilisé pour assurer la prise en charge des utilisateurs du portail.

2.1.5 Événements récents majeurs

Le menu **Événements récents majeurs** affiche les 20 derniers événements enregistrés par l'application one-X Portal for IP Office. Il peut s'agir d'actions effectuées par le service one-X Portal for IP Office ou d'actions d'administration, telles que la connexion/déconnexion d'un administrateur, la modification du mot de passe administrateur, les modifications apportées aux fournisseurs et la restauration de la configuration.

La liste comprend également les tentatives de connexion utilisateur échouées si plus de 10 échecs se produisent au cours d'une période de 5 minutes. Les tentatives de connexion échouées sont basées sur le nom d'utilisateur. Les échecs de connexion à Avaya Communicator ne sont pas pris en compte.

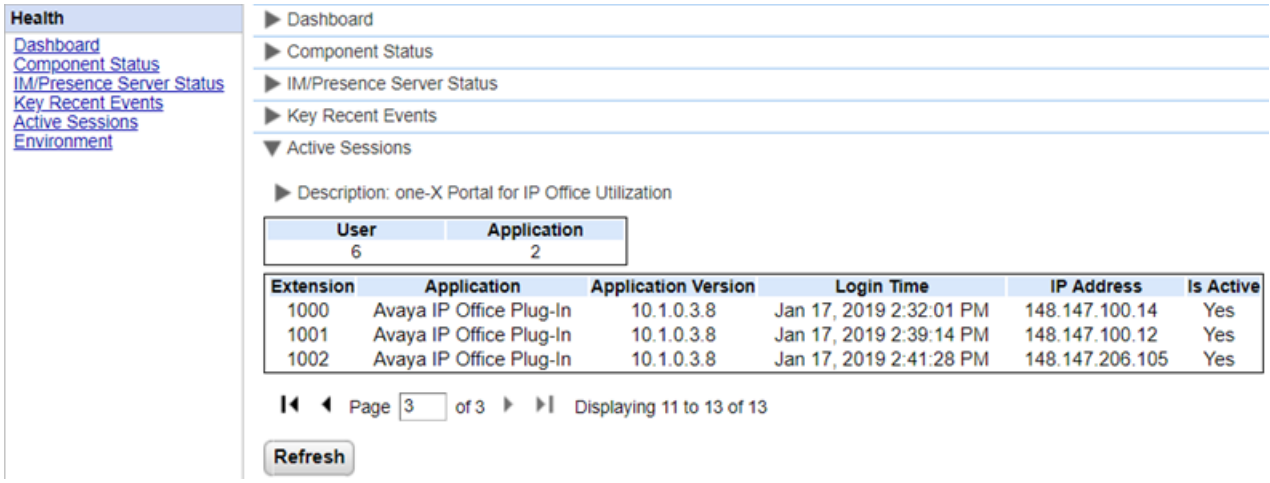


Pour afficher les événements récents majeurs :

1. Sélectionnez **Santé**, puis **Evénements récents majeurs**. Cliquez sur **Actualiser**.
2. Cliquez sur **Obtenir tout** pour récupérer les enregistrements d'événements figurant dans la base de données de one-X Portal for IP Office.
3. Utilisez les commandes de la page pour faire défiler les enregistrements.
4. L'option **Supprimer** supprime l'enregistrement d'état, sans affecter le composant. Les cases à cocher et l'option **Supprimer les sélections** peuvent servir à effacer plusieurs enregistrements.

2.1.6 Sessions actives

Le menu **Sessions actives** affiche le nombre de sessions de navigateur actuellement connectées au serveur one-X Portal for IP Office.

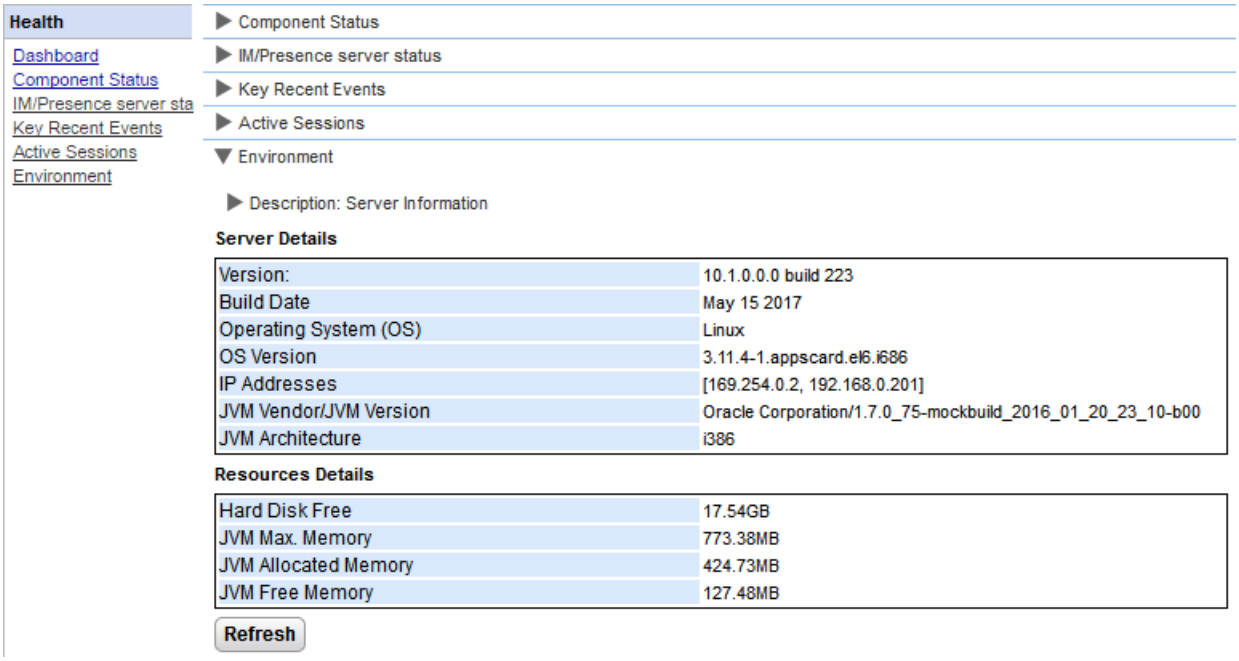


Pour afficher les sessions actives :

1. Sélectionnez **État d'intégrité**, puis **Sessions actives**.
2. Pour mettre à jour les détails, cliquez sur **Actualiser**.

2.1.7 Environnement

Le menu **Environnement** affiche des informations sur le PC du serveur one-X Portal for IP Office. Les informations disponibles dépendent du type du serveur de portail.



Pour afficher les informations sur l'environnement :

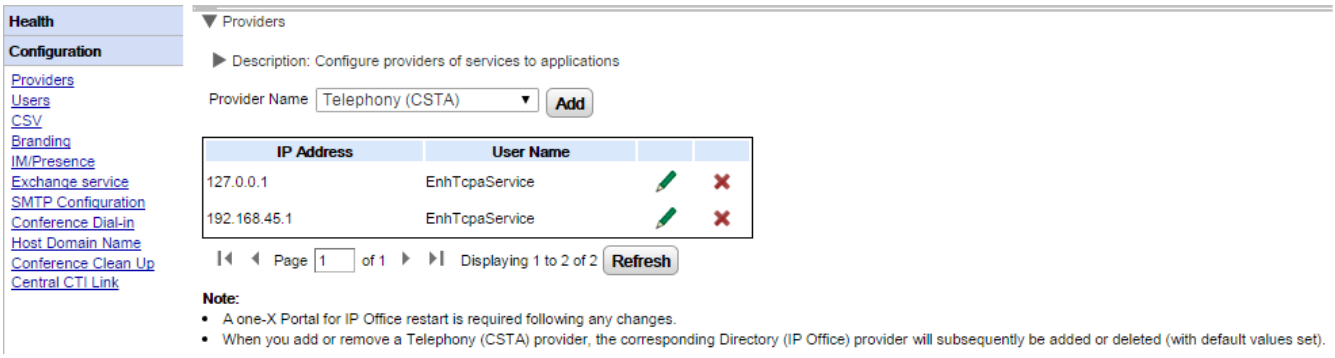
1. Sélectionnez **État d'intégrité**, puis **Environnement**.
2. Cliquez sur **Actualiser**.

2.2 Configuration

Cette section vous permet d'afficher et de vérifier plusieurs options de configuration.

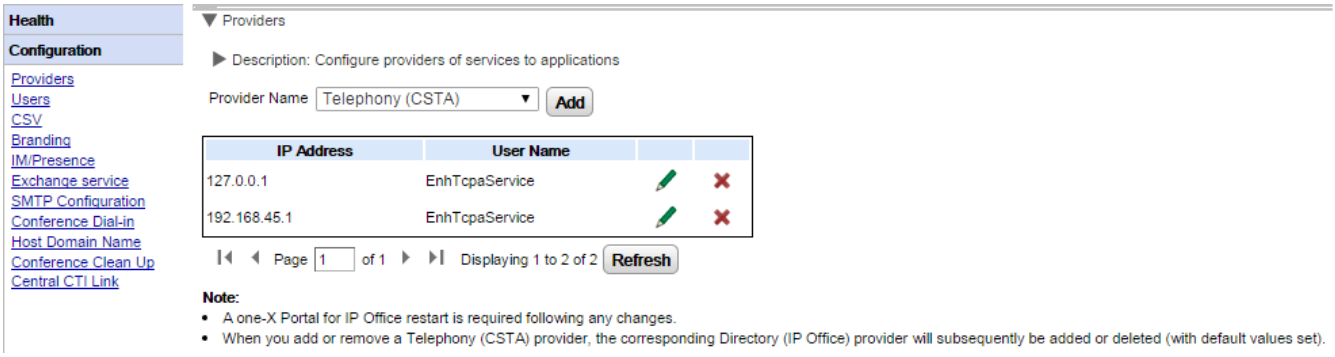
2.2.1 Fournisseurs

Ce menu affiche les fournisseurs de service configurés sur le serveur one-X Portal for IP Office. Le menu **Fournisseurs** permet de modifier les systèmes IP Office et les serveurs LDAP attribués aux fournisseurs.



2.2.1.1 Fournisseur Téléphonie (CSTA)

Les paramètres ci-dessous s'affichent pour les fournisseurs de type Téléphonie (CSTA). Changez-les uniquement si vous maîtrisez bien les procédures d'installation et d'utilisation de one-X Portal for IP Office.

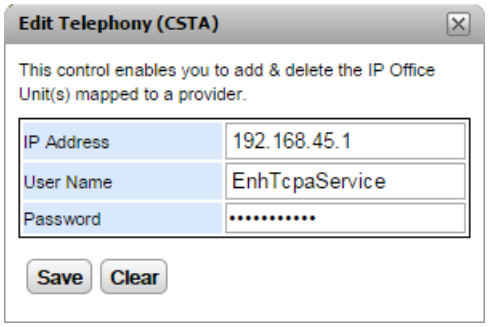


Pour ajouter un nouveau fournisseur CSTA, cliquez sur **Ajouter**. Les paramètres du fournisseur s'affichent. Veuillez noter que l'ajout d'un nouveau fournisseur CSTA ajoute automatiquement un nouveau fournisseur DMSL sous la même adresse. L'ajout d'un nouveau fournisseur est uniquement nécessaire dans un réseau sans configuration centralisée 33.

Pour modifier un fournisseur CSTA existant, cliquez sur l'icône de modification  située à côté de l'entrée existante. Les paramètres du fournisseur s'affichent. Pour ajouter

Paramètres de fournisseur CSTA

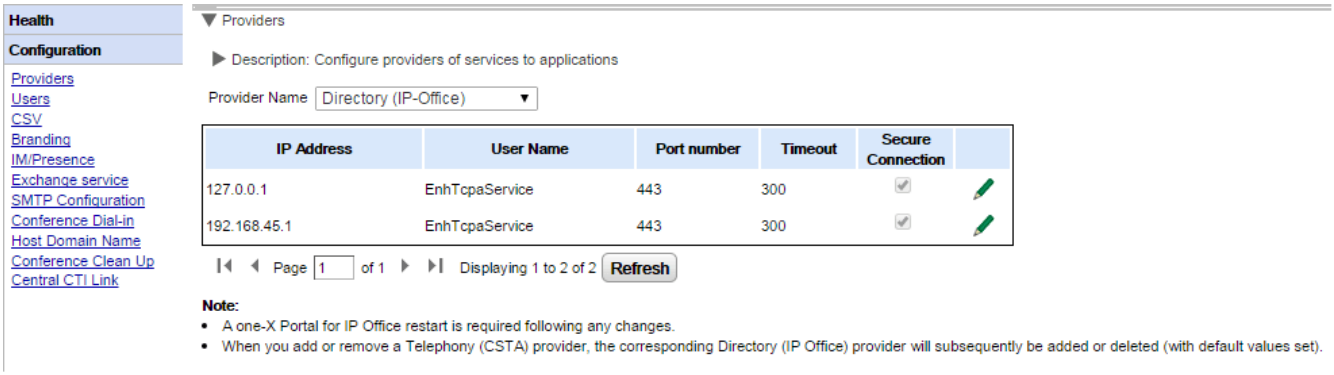
À chaque fois que vous modifiez les paramètres du fournisseur, vous devez redémarrer le service de portail 52.



- **Adresse IP**
  L'adresse IP du système IP Office.
- **Nom d'utilisateur**
  Le nom de l'utilisateur du service TCPA configuré dans les paramètres de sécurité du système IP Office. Par défaut, l'utilisateur est ***EnhTcpaService***.
- **Mot de passe**
  Le mot de passe défini pour l'utilisateur du service TCPA.

2.2.1.2 Fournisseur d'annuaire (IP Office)

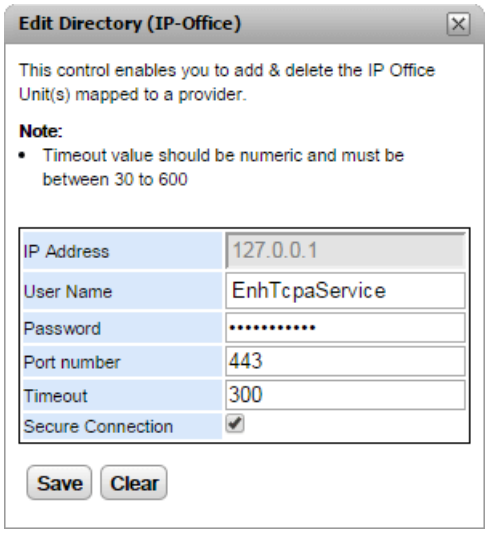
Les paramètres ci-dessous s'affichent pour les fournisseurs d'annuaire (IP-Office). Changez-les uniquement si vous maîtrisez bien les procédures d'installation et d'utilisation de one-X Portal for IP Office.



Pour ajouter un nouveau fournisseur d'annuaire, utilisez les options pour ajouter un fournisseur CSTA20. Pour ajouter un fournisseur existant, cliquez sur l'icône de modification située à côté de l'entrée existante.

Paramètres de fournisseur d'annuaire

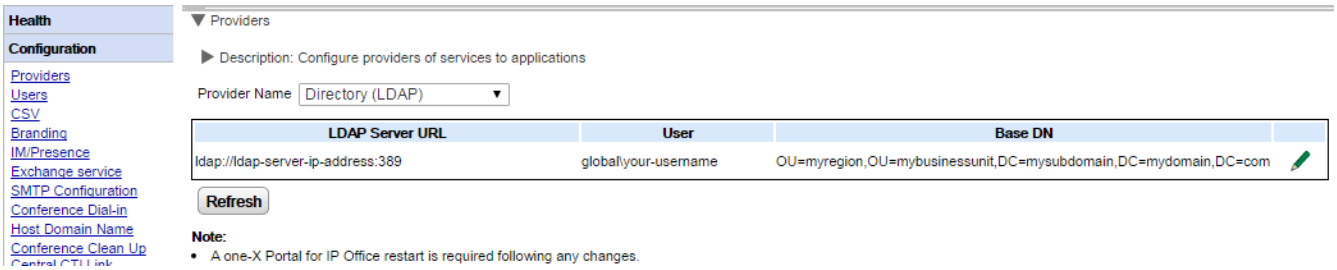
À chaque fois que vous modifiez les paramètres du fournisseur, vous devez redémarrer le service de portail52.



- **Adresse IP**
  L'adresse IP du système IP Office.
- **Nom d'utilisateur**
  Le nom de l'utilisateur du service TCPA configuré dans les paramètres de sécurité du système IP Office. Par défaut, l'utilisateur est ***EnhTcpaService***.
- **Mot de passe**
  Le mot de passe défini pour l'utilisateur du service TCPA.
- **Numéro de port**
  Le numéro du port sur lequel le système IP Office accepte les connexions.
- **Temporisation**
  La valeur de la temporisation, comprise entre 30 et 600 secondes.
- **Connexion sécurisée**
  Permet de se connecter au service d'annuaire du système téléphonique.

2.2.1.3 Fournisseur DSML (LDAP)

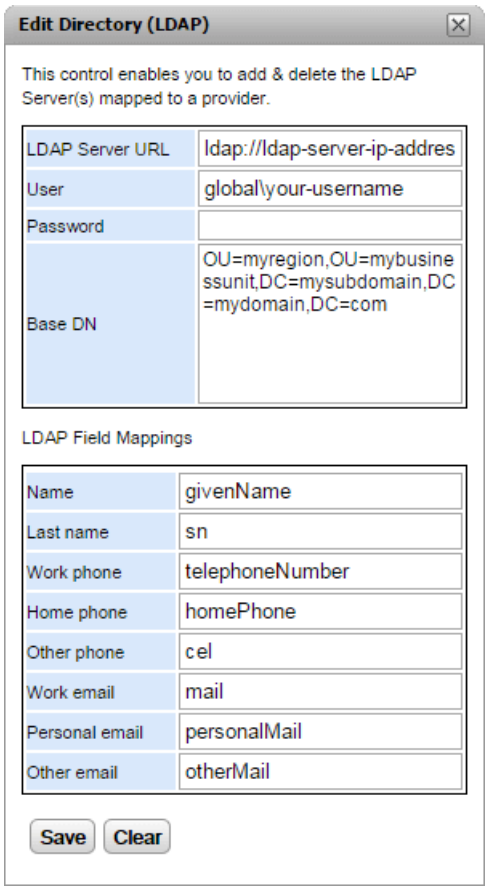
Les paramètres ci-dessous s'affichent pour un fournisseur de type **Répertoire (DSML LDAP)**.



Pour modifier le fournisseur, cliquez sur l'icône de modification .

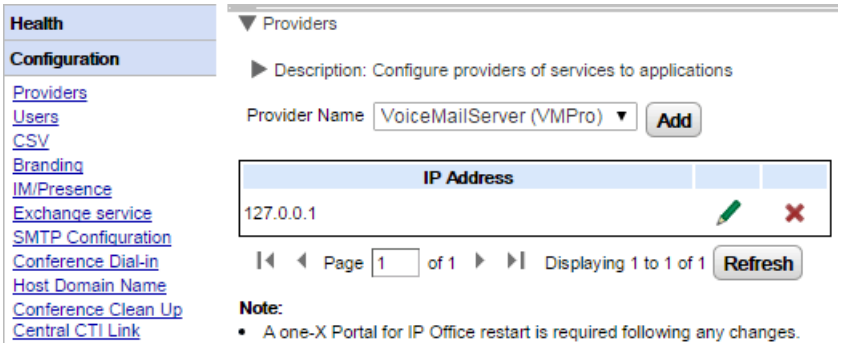
Paramètres de fournisseur LDAP

À chaque fois que vous modifiez les paramètres du fournisseur, vous devez redémarrer le service de portail 52.



2.2.1.4 Fournisseur de messagerie vocale

Les paramètres ci-dessous s'affichent pour un fournisseur **serveur de messagerie vocale**.



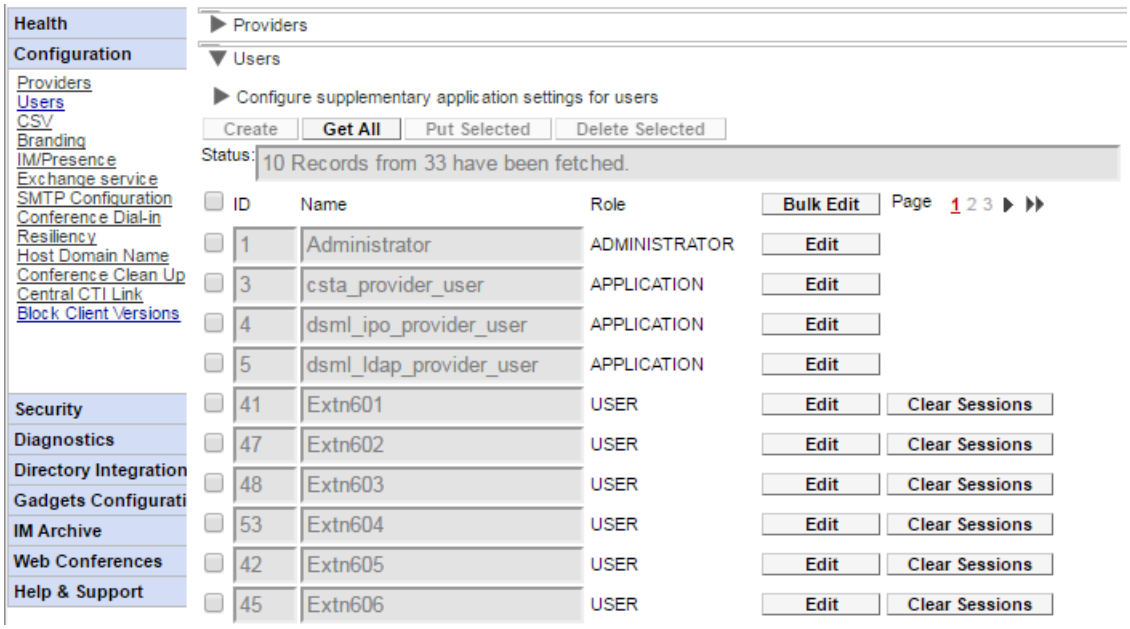
Pour modifier le fournisseur, cliquez sur l'icône de modification .

À chaque fois que vous modifiez les paramètres du fournisseur, vous devez redémarrer le service de portail 52.

2.2.2 Utilisateurs

Vous pouvez voir les utilisateurs d'IP Office dans le menu **Utilisateurs**. Tous les utilisateurs d'IP Office figurent dans la liste, pas seulement ceux qui sont activés pour pouvoir utiliser one-X Portal for IP Office. Veuillez noter qu'en temps normal, le serveur du portail resynchronise sa liste d'utilisateurs connus avec le système téléphonique toutes les 5 minutes.

Vous pouvez modifier certains des paramètres utilisateur enregistrés dans one-X Portal for IP Office ; voir Modification des paramètres utilisateur 66. Vous ne pouvez pas modifier les paramètres utilisateur enregistrés dans IP Office.

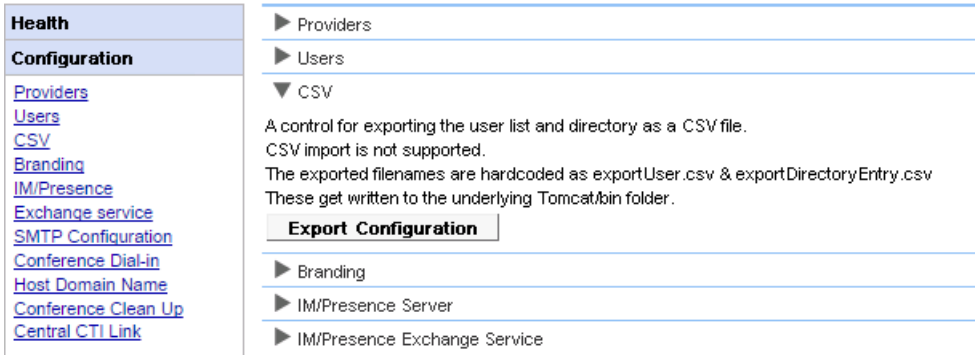


Pour afficher les utilisateurs :

1. Cliquez sur **Configuration**, puis sélectionnez **Utilisateurs**.
2. Cliquez sur **Obtenir tout**.
3. Le bouton **Effacer les sessions** en regard de chaque utilisateur peut être utilisé pour déconnecter tous les clients actuellement connectés que l'utilisateur aurait exécutés.

2.2.3 CSV

Ce menu permet d'exporter les informations des utilisateurs et les répertoires système utilisés par le serveur one-X Portal for IP Office dans des fichiers au format .csv.

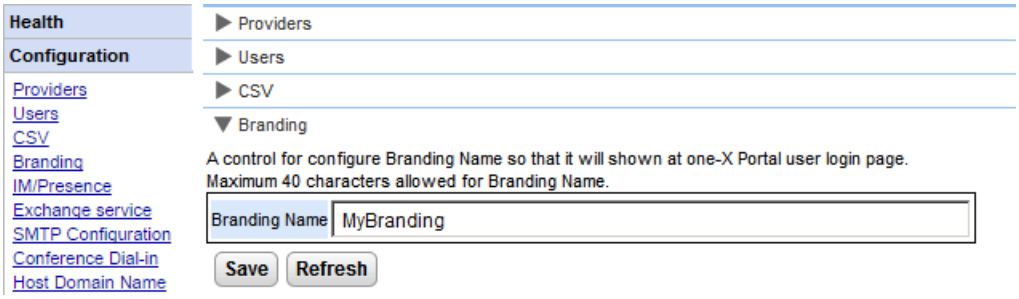


Pour exporter :

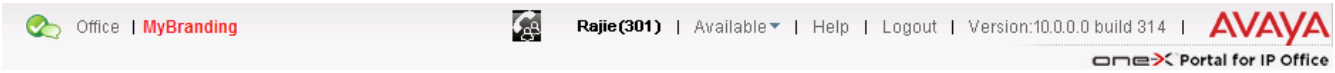
1. Sélectionnez **Configuration**, puis **CSV**.
2. Cliquez sur **Exporter la configuration**.
3. Deux fichiers sont créés dans le sous-dossier ***/bin*** du répertoire de l'application. Pour les serveurs basés sur Linux par défaut avec un chemin similaire à ***/opt/Avaya/oneXportal/10.1.0_136//apache-tomcat/bin***.
   - ***exportUser.csv***
   - ***exportDirectoryEntry.csv***

2.2.4 Personnalisation

Ce menu permet d'ajouter du texte qui est ensuite affiché sur les pages one-X Portal for IP Office une fois qu'un utilisateur est connecté.

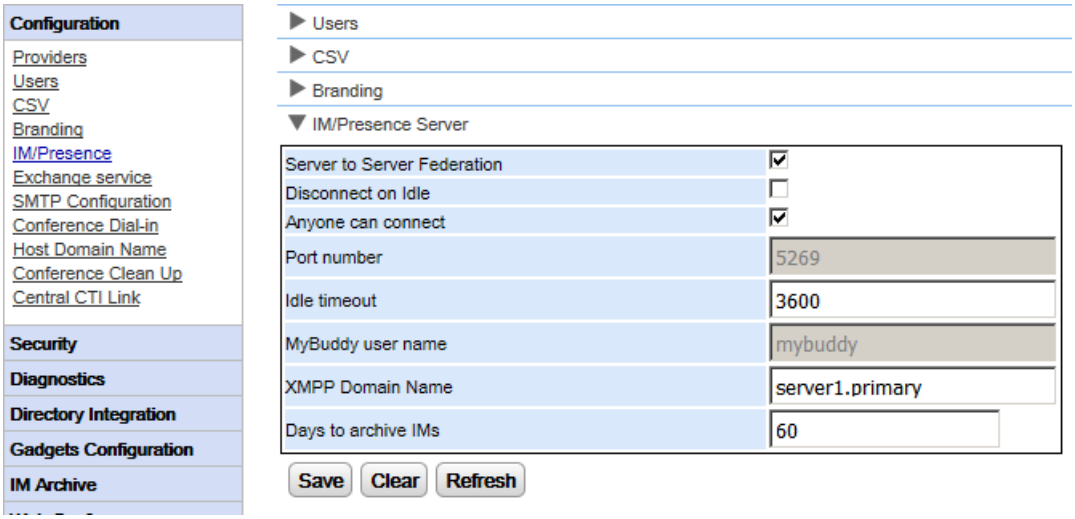


Le texte apparaît dans la barre titre one-X Portal for IP Office comme indiqué ci-dessous.



2.2.5 MI/Présence

Le portail comprend un composant qui agit comme son serveur de messagerie instantanée/de présence. Le serveur de messagerie instantanée/présence peut être configuré séparément. Voir Serveur de messagerie instantanée/présence 76.



Pour configurer le serveur de messagerie instantanée/présence :

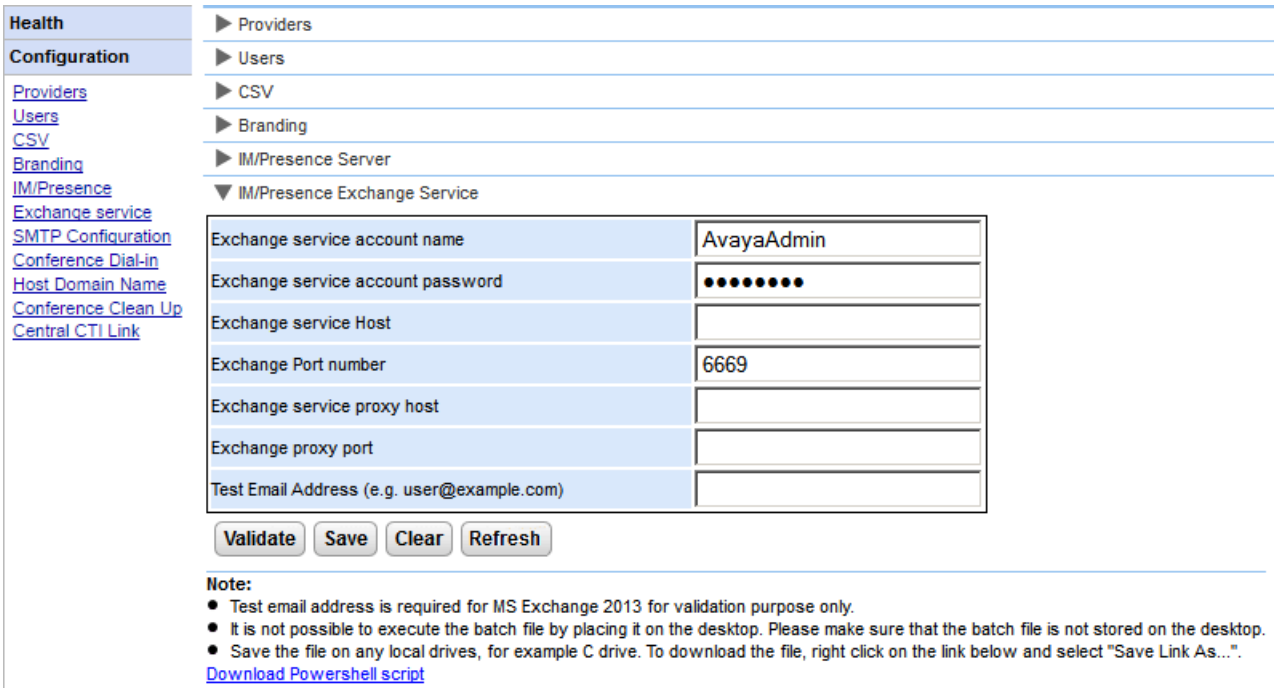
1. Cliquez sur **Configuration** et sélectionnez **Serveur de messagerie instantanée/présence**.
2. Sélectionnez les paramètres serveur requis.
   - **Fédération serveur à serveur**
     Si cette option est sélectionnée, le serveur de présence du portail peut échanger des informations de présence avec d'autres serveurs de présence.
   - **Déconnexion après inactivité**
     Si cette option est activée, les connexions serveur à serveur sont déconnectées si elles restent inactives pendant la période définie dans **Temporisation d'inactivité**.
   - **Tout le monde peut se connecter**
     Permet à tout le monde de se connecter aux services de MI/présence.
   - **Numéro de port**
     Défini sur ***5269***.
   - **Temporisation d'inactivité**
     Durée en seconde définie pour l'option **Déconnexion après inactivité**, si sélectionnée.
   - **Nom d'utilisateur MyBuddy**
     Champ défini sur ***mybuddy***. Cette valeur peut être requise lorsque vous intégrez des informations de présence à d'autres services de MI/présence.
   - **Nom de domaine XMPP**
     Cette option définit le nom de domaine DNS utilisé pour les fonctions de MI/présence :
     - Le nom de domaine XMPP doit être un nom de domaine que le DNS peut résoudre. Vous pouvez définir le nom de domaine XMPP à tout moment. Le nom de domaine doit être accessible depuis Internet si vous souhaitez utiliser la présence en dehors du réseau LAN, par exemple avec one-X Mobile.
     - Avaya recommande l'utilisation d'un serveur DNS partagé de façon à résoudre le nom de votre serveur LAN dans une adresse IP publique du NAT ou du pare-feu, alors qu'il est résolu dans l'adresse IP privée du serveur sur le LAN à l'intérieur de votre réseau.
     - Si vous ne parvenez pas à définir un nom de domaine DNS pouvant être résolu, vous pouvez utiliser l'adresse IP du serveur one-X Portal for IP Office à des fins de MI/présence internes uniquement. Dans ce cas, one-X Portal for IP Office ne peut pas s'associer à des serveurs distants.
     - Pour les serveurs basés sur Linux (IP Office Server Edition, IP Office Application Server et Unified Communications Module), vous devez utiliser les menus Web Control de ces derniers pour configurer leurs paramètres réseau de façon à ce que le lien contenu dans l'e-mail de configuration automatique utilise le nom de domaine FQDN au lieu de l'adresse IP du serveur. Dans Web Control, accédez à Paramètres > Système > Nom de l'hôte pour modifier les paramètres réseau. Si vous modifiez le nom de domaine de toute autre manière, les liens e-mail risquent de ne pas fonctionner correctement.

- **Nombre de jours d'archivage MI**
  Ce champ permet de définir la durée de conservation des messages dans l'archive MI avant leur suppression. La valeur par défaut est 182 jours (6 mois). Si nécessaire, vous pouvez désactiver l'archivage MI 83 à l'aide de la console d'administration XMPP. Le serveur de présence/MI doit être disponible (voir État du serveur de présence/MI 15) pour modifier ce paramètre.

3. Cliquez sur **Enregistrer**.

2.2.6 Service Exchange

one-X Portal for IP Office peut être configuré avec le serveur Exchange pour exploiter l'exploration de calendrier et les informations de présence des utilisateurs.

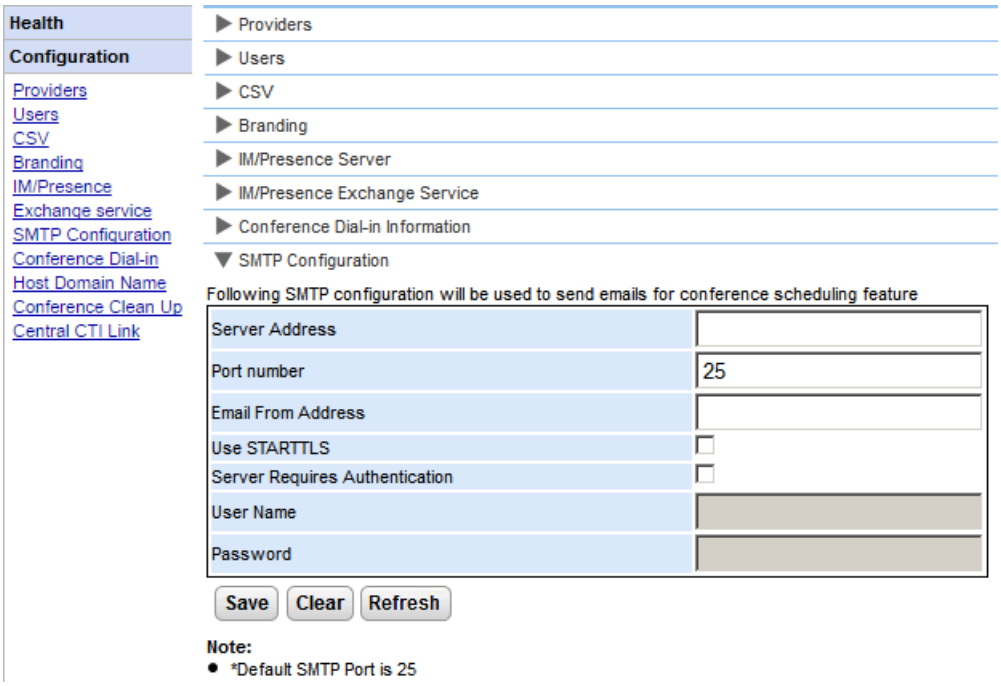


Pour configurer les services Exchange :

1. Cliquez sur **Configuration** dans le volet de navigation gauche.
2. Cliquez sur **Service Exchange**.
   a. Entrez ***AvayaAdmin*** comme **nom de compte service Exchange**. Assurez-vous que ce nom soit le même que pour le compte ***AvayaAdmin*** que vous avez créé sur le serveur d'échange.
   b. Entrez le mot de passe qui a été défini pour **AvayaAdmin** comme **mot de passe de compte service Exchange**.
   c. Entrez l'adresse IP de l'hôte du service Exchange dans **Hôte de service Exchange**.
   d. Entrez le numéro de port du service Exchange dans **Numéro du port Exchange**.
   e. Entrez le nom de domaine du serveur proxy utilisé pour connecter le serveur Exchange dans **Hôte proxy du service Exchange**.
   f. Entrez le numéro de port du serveur proxy pour le service Exchange dans **Port proxy Exchange**.
   g. Définissez une **adresse de messagerie électronique d'essai** valide.
3. Cliquez sur **Valider la configuration du service Exchange** pour savoir si les informations Exchange fournies sont valides.
4. Cliquez sur **Enregistrer**.

2.2.7 Configuration SMTP

Les invitations à des conférences destinées aux utilisateurs peuvent être envoyées par messagerie instantanée ou électronique. Pour un envoi par e-mail, les paramètres associés doivent être configurés ci-dessous. L'adresse e-mail associée à chaque participant est définie dans la configuration du système téléphonique.

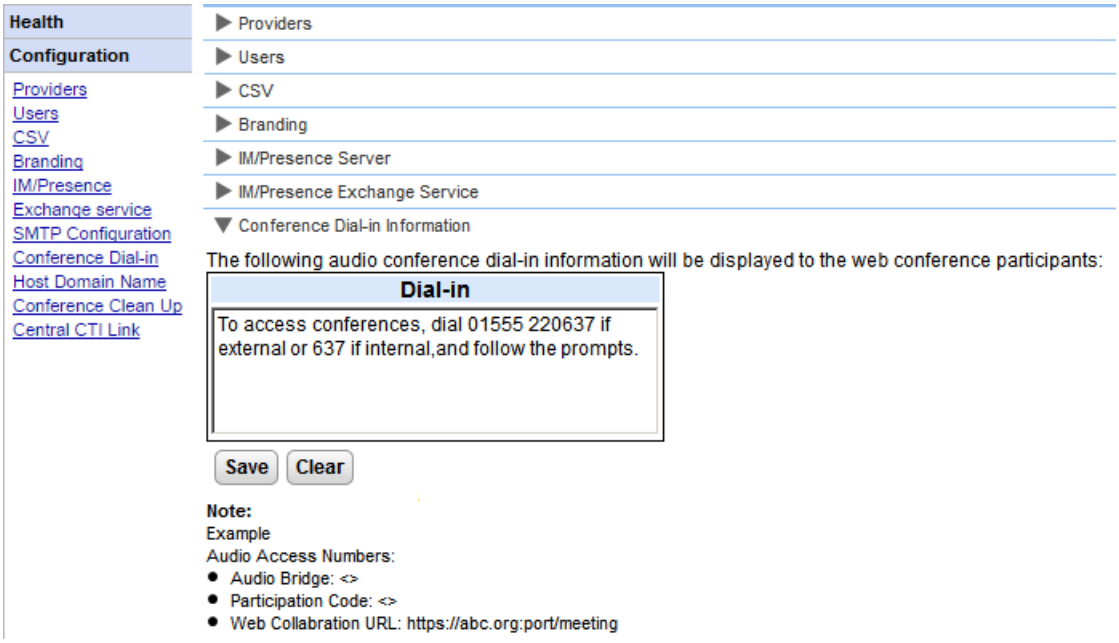


Pour définir le texte de notification :

1. Sélectionnez **Configuration**, puis **Configuration SMTP**.
2. Indiquez les détails e-mail SMTP dont le serveur a besoin :
   - **Adresse du serveur**
     Adresse IP du serveur SMTP du client.
   - **Numéro de port**
     Port d'écoute SMTP du serveur. La valeur par défaut est 25.
   - **Adresse de courrier électronique d'origine**
     Adresse utilisée par le serveur. Certains serveurs ne feront que relayer des messages provenant d'adresses reconnues ou d'adresses du même domaine.
   - **Utiliser STARTTLS**
     Sélectionnez ce champ pour activer l'encodage TLS/SSL. L'encodage permet l'intégration message vocal-email avec des fournisseurs d'emails hébergés qui autorisent uniquement SMTP sur un acheminement sécurisé.
   - **Le serveur doit être authentifié**
     Si le serveur nécessite un compte utilisateur pour recevoir et envoyer des courriers électroniques, saisissez les informations sur le compte configuré sur ce serveur pour qu'IP Office puisse s'en servir.
     - **Nom d'utilisateur**
       Nom de compte à utiliser si l'option Le serveur doit être identifié est sélectionnée.
     - **Mot de passe**
       Mot de passe à utiliser si l'option Le serveur doit être identifié est sélectionnée.
3. Cliquez sur **Enregistrer**.

2.2.8 Accès distant à une conférence

Quand un utilisateur programme une conférence, le serveur envoie une notification aux participants conviés par messagerie électronique ou instantanée. Cette notification inclut les détails de la conférence définie par l'utilisateur (numéro de pont, code du participant). Elle peut également comprendre le texte fixe qui a été défini via le menu **Accès entrant conférence**.



Pour définir le texte de notification :

1. Sélectionnez **Configuration**, puis **Accès entrant conférence**.
2. Saisissez le texte fixe à inclure dans toutes les notifications de conférence.
3. Cliquez sur **Enregistrer**.

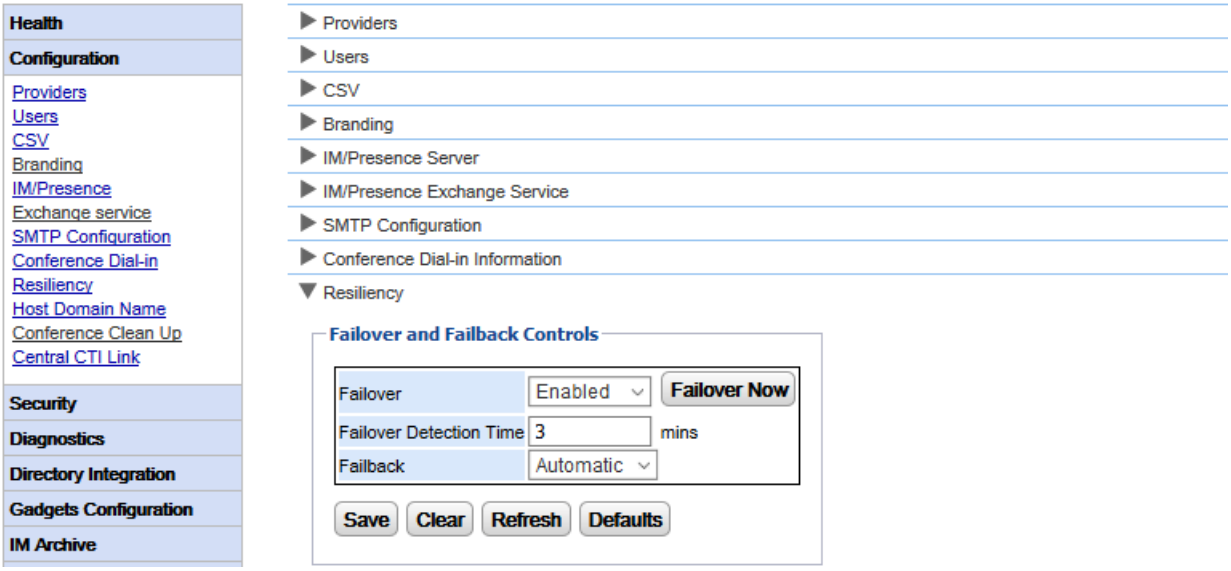
2.2.9 Résilience

Ce menu est disponible sur les serveurs de portail sous Linux qui prennent en charge un réseau IP Office Server Edition Select. Il fournit des paramètres supplémentaires pour le serveur de portail, qui sont nécessaires pour en contrôler la résilience. Voir Résilience 57.

- Sur les systèmes existants en mode de non sélection basculés vers le mode IP Office Server Edition Select, un redémarrage des services du portail peut être requis afin que les paramètres de résilience soient disponibles. De même, il peut être nécessaire de redémarrer les service de portail après la première configuration de la résilience de portail lors de la configuration du système IP Office.

Paramètres du serveur principal

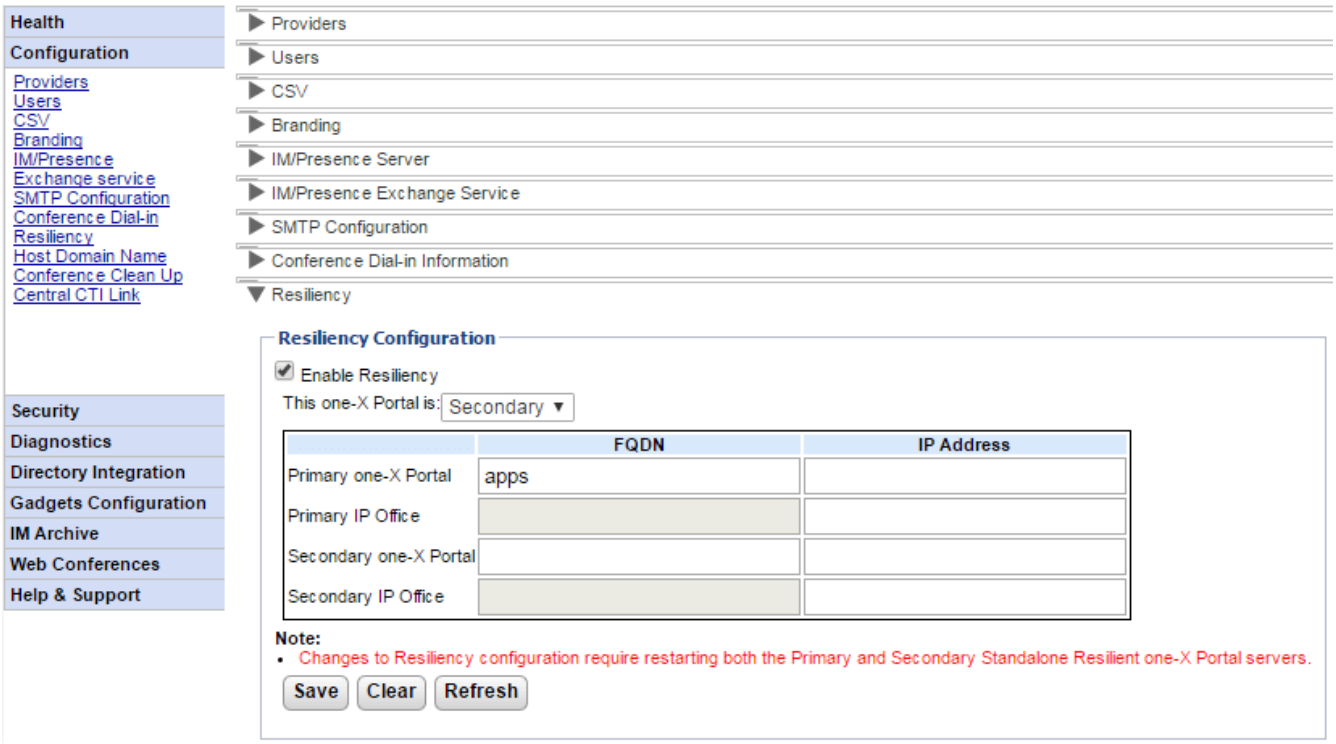
Les paramètres affichés sur le serveur principal sont les suivants :



- **Basculement**
  Sélectionnez cette option si le serveur doit prendre en charge le basculement. Si l'option est activée, le nom de domaine du serveur de portail secondaire doit être défini dans le formulaire Nom de domaine de l'hôte 32.
  - **Basculement maintenant**
    Cette commande peut être utilisée pour lancer manuellement le processus de basculement.
- **Délai de détection de basculement**
  Définit le délai en minutes avant le basculement lorsque des problèmes potentiels sont détectés. La valeur par défaut (3 minutes) cesse le basculement, qui est déclenché par des redémarrages de maintenance habituels.
- **Reprise**
  Définit si le processus de reprise doit être lancé de façon automatique lorsque l'opportunité se présente. Si vous choisissez l'option Manuel, un redémarrage des services de portail est requis afin de terminer le basculement.

Paramètres du serveur d'applications

Ces paramètres apparaissent également sur un serveur d'applications. Lorsqu'un serveur est utilisé sur un réseau IP Office Server Edition Select, il peut agir en tant que serveur de portail pour le serveur principal ou secondaire, en remplaçant le service de portail intégré sur ce serveur.

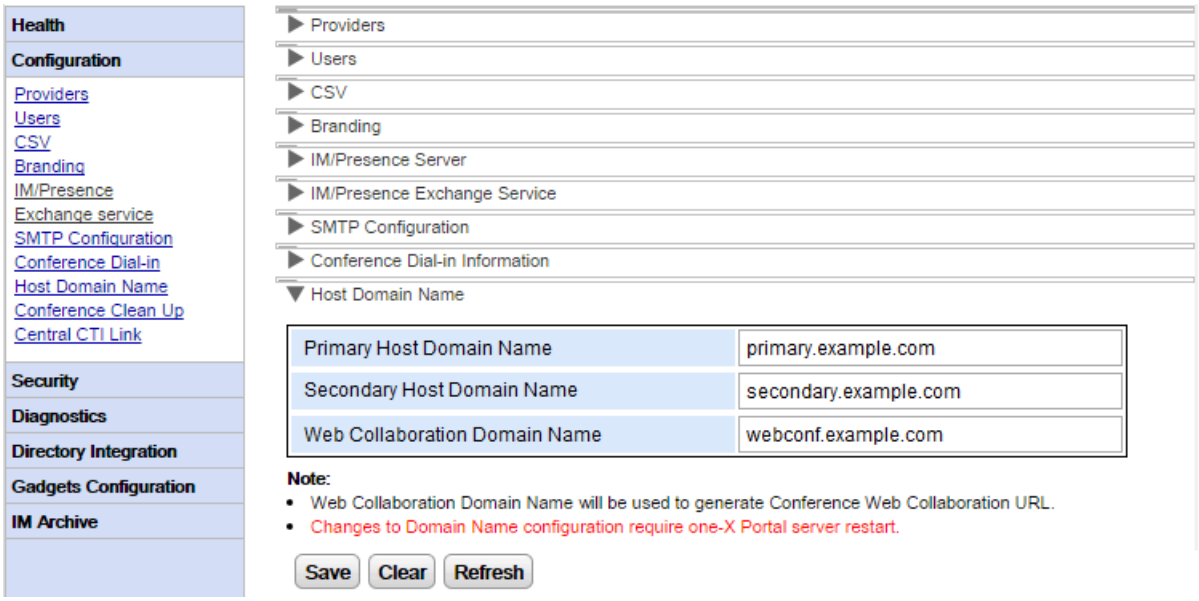


- **Activer la résilience**
  Lorsque cette option est sélectionnée, elle active la résilience du portail et affiche les champs supplémentaires requis pour définir les adresses des autres serveurs inclus dans la configuration de la résilience et le rôle de ces serveurs. Si la résilience n'est pas activée, le service de portail du serveur secondaire est automatiquement arrêté et ne peut pas être redémarré manuellement.
  - **Ce one-X Portal :**
    Définissez le rôle de ce serveur.
    - **Principal**
      Sélectionnez cette option si ce serveur doit servir de serveur de portail principal.
    - **Secondaire**
      Sélectionnez cette option si ce serveur doit servir de serveur de portail de sauvegarde/remplacement au cas où le portail principal n'est pas disponible.
- **Adresse IP/FQDN**
  Utilisez ce tableau pour saisir les noms de domaine complets ou les adresses IP de tous les portails et serveurs IP Office inclus dans la configuration de la résilience.

2.2.10 Nom de domaine de l'hôte

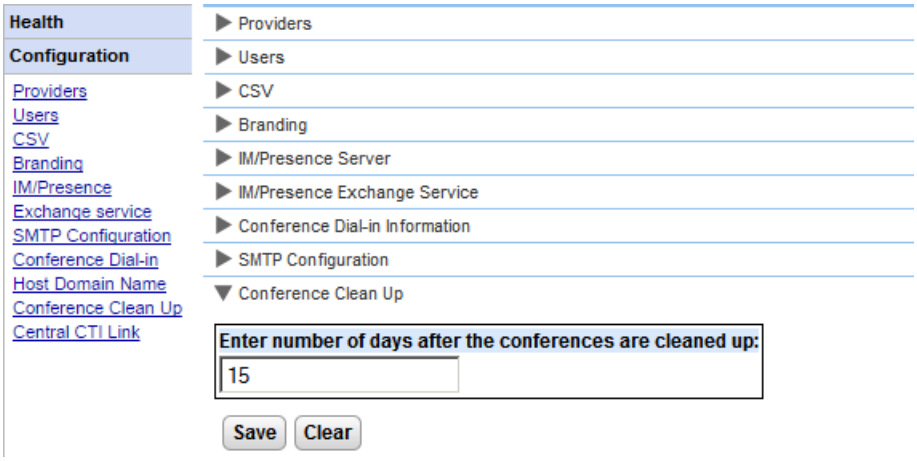
Le menu **Configuration | Nom de domaine hôte** est utilisé pour définir le nom de domaine utilisé pour l'accès aux services de portail et entre les serveurs de portail. Le nombre de noms de domaine requis dépend du type de serveur de portail.

Notez que pour que la modification des noms de domaine soit prise en compte, il faut redémarrer le service de portail.



2.2.11 Nettoyage de conférence

Ce menu permet de configurer le nombre de jours que le serveur doit conserver les informations de la conférence. Cette option n'est pas prise en charge par le serveur Windows.



2.2.12 Lien CTI central

Les serveurs du portail IP Office Server Edition peuvent utiliser le mode CTI centralisé. Dans ce mode, il suffit de lier le service de portail à un seul système IP Office sous Linux pour fournir des services à tous les systèmes IP Office du réseau. Cela inclut un IP Office Application Server utilisé avec IP Office Server Edition.

- Cette option n'est pas disponible pour les serveurs basés sur les serveurs basés sur UCM et un IP Office Application Server prenant en charge une unité IP500 V2.

En mode CTI centralisé, le service de portail fournit automatiquement des services d'appel à tous les systèmes IP Office du réseau. Il obtient les entrées des répertoires système de tous les systèmes et automatiquement celles des systèmes ajoutés ou supprimés du réseau. En outre, le portail obtient automatiquement les informations concernant le serveur de messagerie vocal central.

- **Lien CTI central**
  Ce paramètre est utilisé pour activer ou désactiver le mode CTI centralisé. Veuillez noter que vous devrez redémarrer le service one-X Portal for IP Office en cas de modification de ce paramètre.
  - **S'il est activé :**
    Lorsque ce paramètre est activé, le service de portail utilise le mode CTI centralisé. Cela signifie que :
    - Le portail se connecte à un seul système IP Office. Les fournisseurs CSTA et DSML sont uniquement créés pour ce système. Toutefois, les connexions à ce système sont utilisées pour détecter et fournir des services à tous les autres systèmes IP Office du réseau.
    - La liaison vers le système IP Office permet également de découvrir les paramètres du serveur de messagerie vocale et de créer automatiquement le fournisseur nécessaire.
    - Si la résilience IP Office Server Edition 57 est également activée, les fournisseurs CSTA sont alors créés pour le système IP Office principal, de même que pour les systèmes IP Office secondaires.
    - Chaque système IP Office individuel que le serveur de portail a détecté est toujours affiché dans le menu **État du composant** 15.
    - Le portail obtient les informations sur le serveur IP Office et les annuaires système depuis le système IP Office principal.
    - Les enregistrements des annuaires personnels sont toujours obtenus à partir du système IP Office hôte de chaque utilisateur.
  - **S'il est désactivé :**
    Lorsque ce paramètre n'est pas activé :
    - Les fournisseurs CSTA et DSML doivent être configurés manuellement pour chaque système IP Office du réseau. Cette opération se fait au cours de l'installation et/ou via les menus **Fournisseurs** 19. Toutefois, le fournisseur de messagerie vocale est mis en service automatiquement en fonction des informations transmises par le système IP Office connecté.
    - Il s'agit du paramètre par défaut pour les systèmes mis à niveau vers IP Office version 10.

Mise en service automatique

Les systèmes mis à niveau à partir de la version 9.1 affichent et utilisent leur paramètre **Mise en service automatique** original à la place de **Liaison CTI centrale**. Si **Approvisionnement automatique** est activé, le fournisseur CSTA initial connecté est utilisé pour créer automatiquement des fournisseurs supplémentaires et maintenir les fournisseurs CSTA et DSML pour tous les autres systèmes du réseau. Dans la version 10.0, le fournisseur de messagerie vocale est également automatiquement configuré à l'aide des informations du système téléphonique.

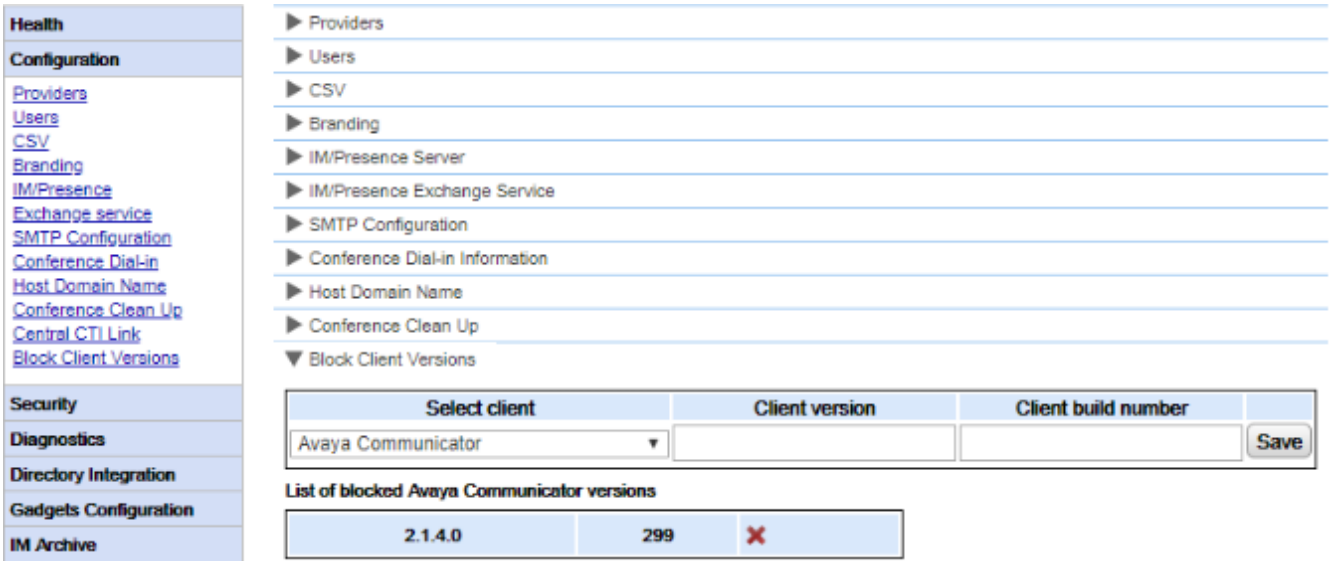
Les systèmes qui utilisent **Mise en service automatique** peuvent être convertis pour utiliser **Liaison CTI centrale**, en cliquant sur le bouton **Convertir en Liaison CTI centrale**. Cette procédure ne peut être annulée.

2.2.13 Bloquer les versions du client

Ce menu peut être utilisé pour créer une liste des versions du client que le serveur de portail ne prend pas en charge. Pour ce faire, il suffit d'ajouter la version et la build du client à la liste des clients bloqués.

Les clients bloqués ne peuvent pas se connecter. Les clients déjà connectés pourront continuer à travailler jusqu'à ce qu'ils se déconnectent.

Pour chaque client, 15 combinaisons version/build au maximum peuvent être bloquées.



Pour ajouter un nouveau client bloqué :

1. Utilisez le menu déroulant **Sélectionner un client** pour sélectionner le client.
2. Saisissez les valeurs numériques de la **Version du client** et de la **Build du client**. Les deux valeurs doivent être définies.
3. Cliquez sur **Enregistrer**.

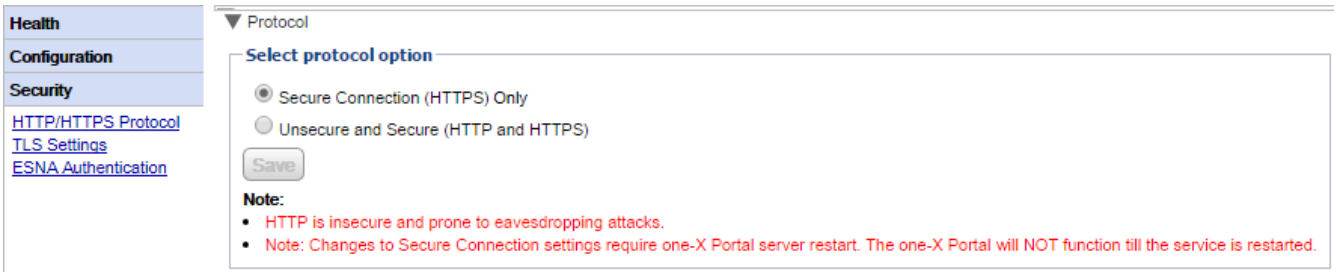
Pour supprimer un client bloqué :

1. Cliquez sur l'icône en forme de croix.

2.3 Sécurité

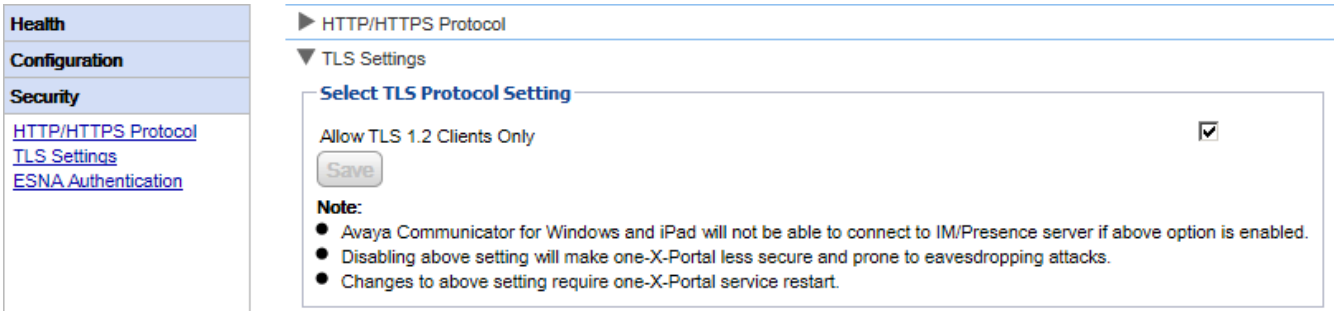
2.3.1 Protocole HTTP/HTTPS

Par défaut, le serveur prend uniquement en charge l'accès HTTPS chiffré lors de l'installation ; c'est-à-dire le port 9443 sur un serveur Linux et le port 8443 sur un serveur Windows. Ce menu permet également d'activer l'accès HTTP sur le port 8080.



2.3.2 Paramètres TLS

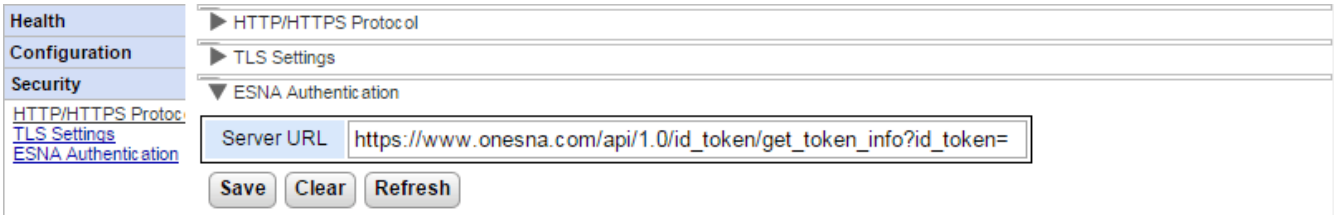
Le serveur de portail prend en charge les utilisateurs et les applications qui se connectent à l'aide de TLS. Cette prise en charge peut toutefois être limitée aux connexions utilisant TLS 1.2.



- **Autoriser les clients TLS 1.2 uniquement**
  Si cette option est activée, la prise en charge TLS du serveur de portail se limite à TLS 1.2. Si vous modifiez ce paramètre, vous devez redémarrer le service de portail 52 pour que la modification soit prise en compte.
  - Notez que les applications clientes d'Avaya Communicator actuelles ne prennent pas en charge TLS 1.2 et ne pourront donc pas se connecter si cette option est activée.

2.3.3 Authentification ESNA

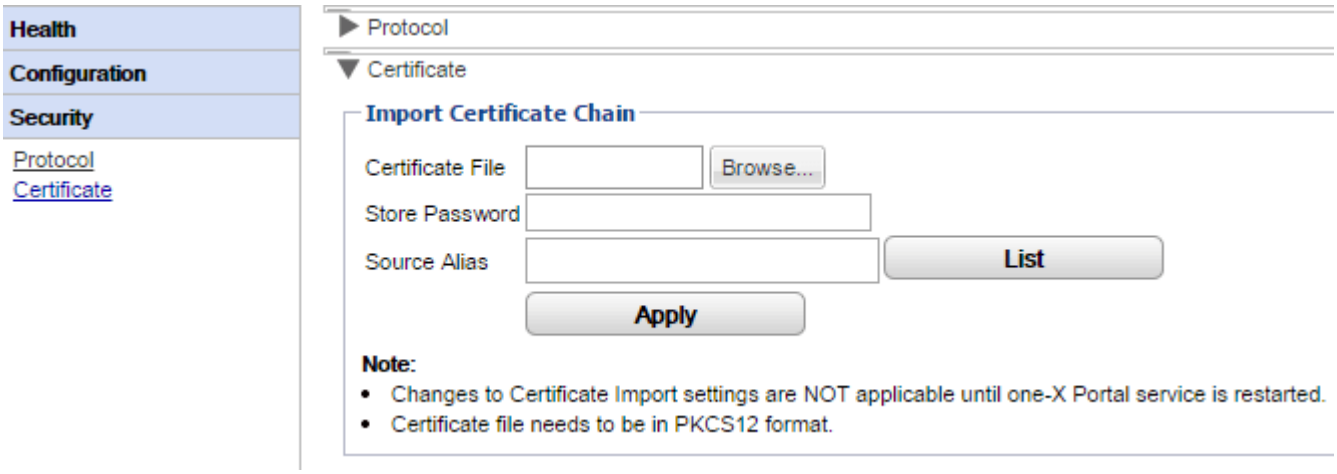
Les utilisateurs qui se connectent à l'aide d'un compte ESNA doivent être authentifiés sur les serveurs d'ESNA.



- **URL du serveur**
  Ce champ contient l'URL qui permet de rediriger les demandes d'authentification des utilisateurs vers ESNA.

2.3.4 Certificat

Ce menu permet au portail d'importer un certificat pour un accès chiffré. Ce certificat est nécessaire pour les applications qui utilisent la connexion TLS chiffrée au portail, par exemple Avaya Communicator.

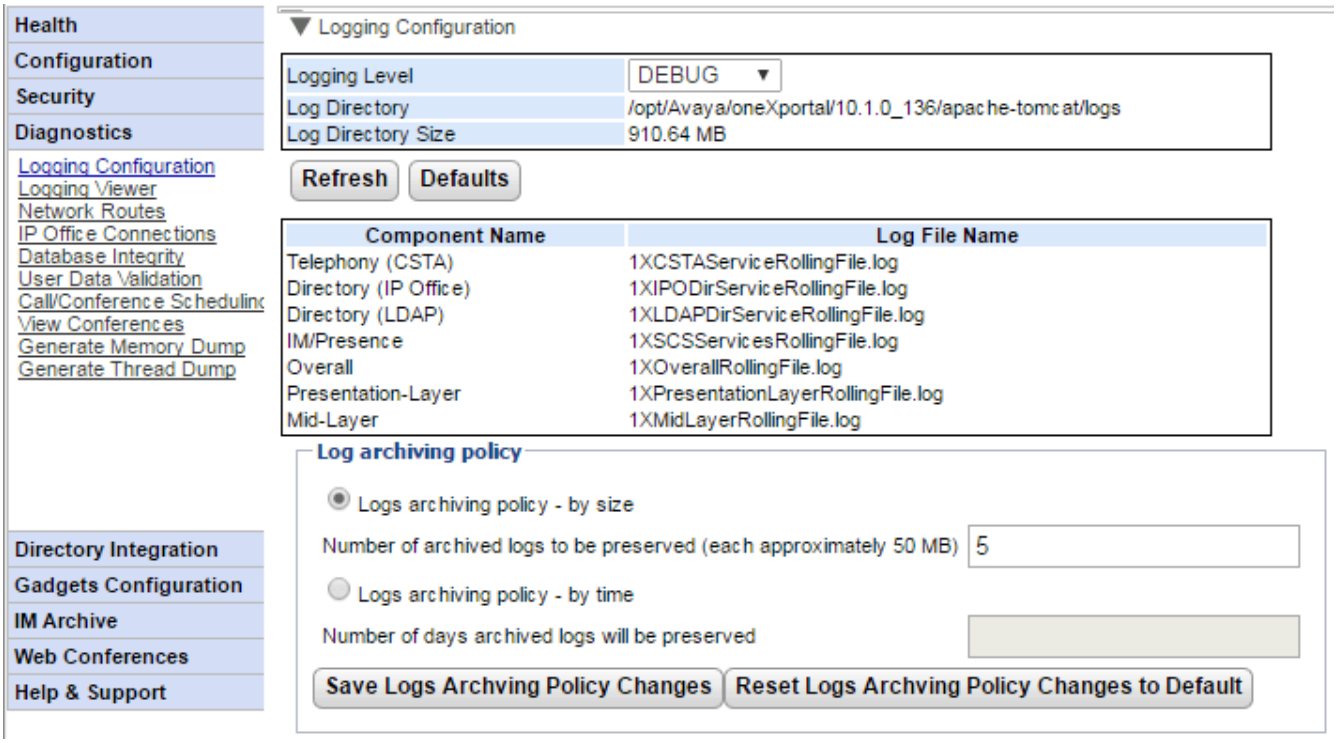


2.4 Diagnostics

Cette section vous permet d'exécuter plusieurs vérifications de diagnostic.

2.4.1 Configuration des journaux

one-X Portal for IP Office prend en charge un grand choix de méthodes de sortie des journaux permettant de choisir le niveau de consignation requis.



- **Niveau de consignation principal**
  Ce champ permet de sélectionner le niveau minimal des événements à consigner ou de désactiver la consignation des événements (pour ce faire, sélectionnez ***DÉSACTIVÉ***).
- **Annuaire de journaux**
  L'annuaire dans lequel le serveur enregistre ses fichiers journaux. Non modifiable.
- **Taille de l'annuaire de journaux**
  La taille totale actuelle des fichiers journaux.
- **Actualiser**
  Cliquez sur ce bouton pour mettre à jour les informations affichées.
- **Défaut**
  Cliquez sur ce bouton pour redonner sa valeur par défaut au niveau de consignation principal. Le paramètre par défaut est ***ERREUR***, sauf sur les serveurs Unified Communications Module où le défaut est ***DÉSACTIVÉ***.
- **Descriptions des fichiers journaux :**
  Ce tableau montre les fichiers journaux utilisés par les différents composants de one-X Portal for IP Office.
  - **Téléphonie (CSTA) :** *1XCSTAServiceRollingFile.log*
    Ce journal capture les informations de téléphonie. Son rôle consiste notamment à obtenir des informations sur les utilisateurs et les licences auprès des systèmes IP Office.
  - **Annuaire (IP-Office) :** *1XIPODirServiceRollingFile.log*
    Ce journal capture les informations sur les répertoires IP Office.
  - **Répertoire (LDAP) :** *1XLDAPDirServiceRollingFile.log*
    Ce journal capture les informations sur le répertoire LDAP.
  - **MI/Présence :** *1XSCSServicesRollingFile.log*
    Ce journal capture les informations sur l'IM et la présence d'IP Office.
  - **Tout :** *1XOverallRollingFile.log*
    Il s'agit d'un fichier journal global contenant tous les types d'événements consignés.
  - **Couche présentation :** *1XPresentationLayerRollingFile.log*
    Ce journal capture les informations sur l'activité du navigateur des utilisateurs.

- **Couche intermédiaire :** *1XMidLayerRollingFile.log*
  Ce journal capture les interactions entre les divers composants one-X Portal for IP Office, y compris les systèmes IP Office.

- **Politique d'archivage des journaux**
  Ces paramètres vous permettent de configurer la conservation des fichiers journaux gérée par le serveur. Par défaut, le serveur conserve les 5 derniers fichiers journaux.

  - **Politique d'archivage des journaux - par taille**
    Si cette option est sélectionnée, le paramètre Nombre de fichiers journaux est utilisé pour déterminer les fichiers à conserver. Lorsqu'un nouveau fichier est ouvert (les fichiers sont automatiquement écrasés lorsqu'ils atteignent environ 50 Mo), le fichier le plus ancien est automatiquement supprimé si le nombre de fichiers à conserver a été dépassé.

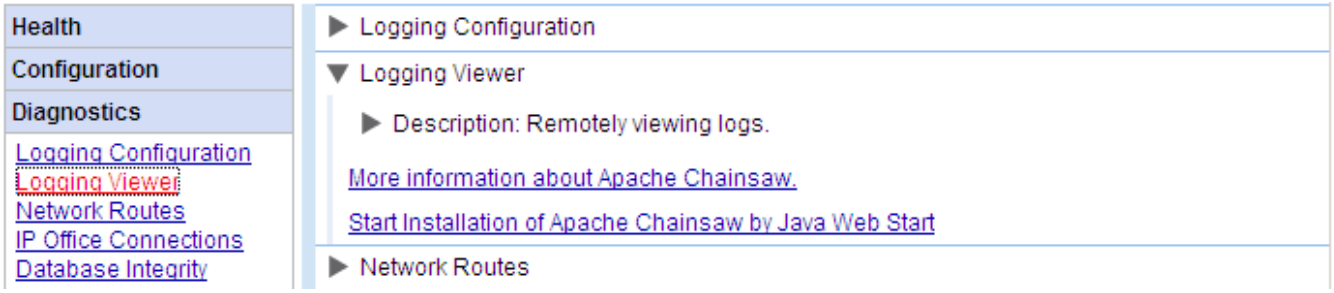
    - **Nombre de journaux archivés à conserver**
      Définit le nombre de fichiers à conserver si **Politique d'archivage des journaux - par taille** est sélectionné. La valeur par défaut est de 5 fichiers.

  - **Politique d'archivage des journaux - par heure**
    Si cette option est sélectionnée, la date du fichier journal est utilisée pour déterminer les fichiers qui seront conservés. Les fichiers les plus anciens sont automatiquement supprimés.

    - **Nombre de jours de conservation des journaux archivés**
      Définit le nombre de jours de conservation d'un fichier journal si **Politique d'archivage des journaux - par heure** est sélectionné. La valeur par défaut est de 5 jours.

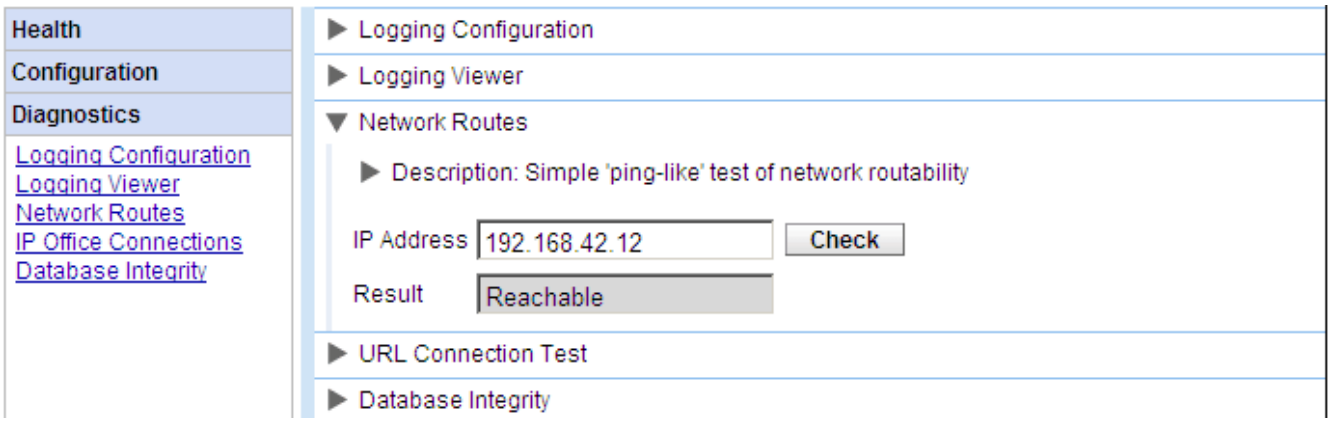
2.4.2 Visionneuse de journaux

Outre la consignation aux fichiers, il est possible de visualiser la sortie des messages de consignation par les composants one-X Portal for IP Office dans une application de consignation à distance prenant en charge le format Log4j. Le menu **Diagnostics | Visionneuse de journaux** contient des liens vers des sites renseignant sur Apache Chainsaw, qui est une application de consignation compatible, et sur son installation 89.



2.4.3 Itinéraires réseau

Ce menu permet de tester le routage entre le serveur one-X Portal for IP Office et une adresse IP Office. Il utilise TCP vers le port 7 (service Echo) sur l'adresse IP cible. Notez que cela ne fonctionne pas avec les unités de contrôle IP Office, pour lesquelles il faut utiliser à la place Connexions IP Office 39.

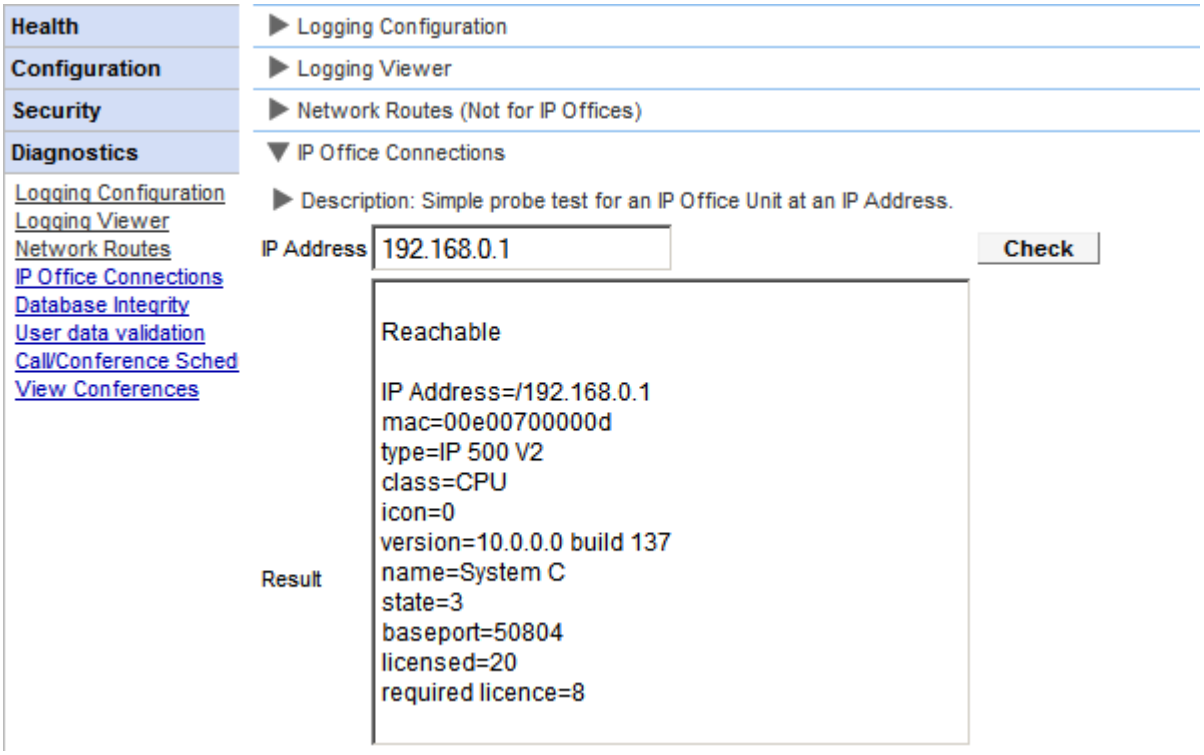


Pour contrôler un itinéraire réseau :

1. Sélectionnez **Diagnostics**, puis **Itinéraires réseau**.
2. Saisissez l'**adresse IP** de la cible, puis cliquez sur **Vérifier**.
3. Le serveur one-X Portal for IP Office indique si la cible se trouve à l'état ***Accessible*** ou ***Inaccessible***.

2.4.4 Connexions IP Office

Ce menu permet de tester la connexion entre le serveur one-X Portal for IP Office et une adresse IP Office particulière. Le test de la connexion fait appel à la méthode de découverte standard utilisée par les applications IP Office, telles que IP Office Manager (connexion au port 50804 de l'unité de contrôle IP Office).

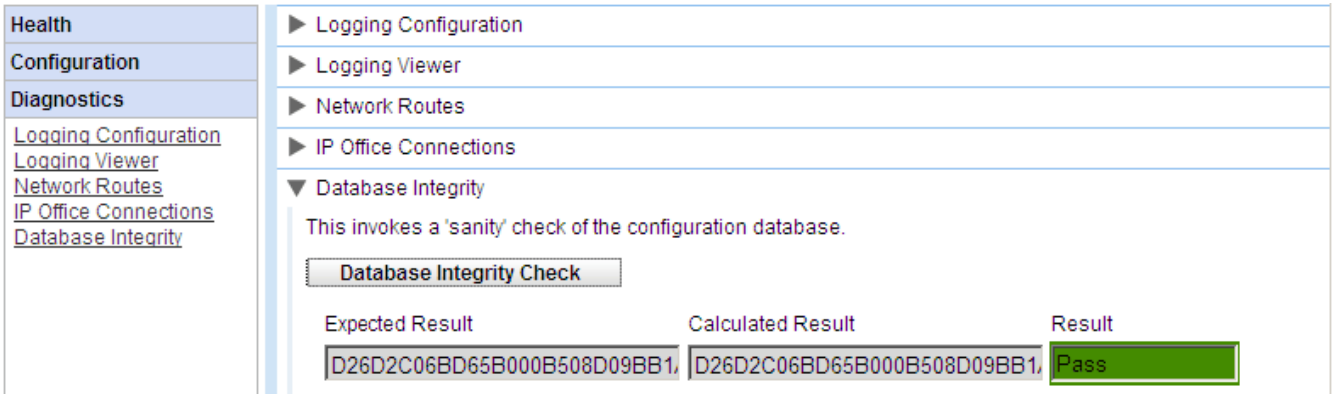


Pour tester la connexion IP Office :

1. Sélectionnez **Diagnostics**, puis **Connexions IP Office**.
2. Saisissez l'**adresse IP** du système IP Office cible, puis cliquez sur **Vérifier**.
3. Si le système IP Office est accessible, les résultats incluent ses informations de base.

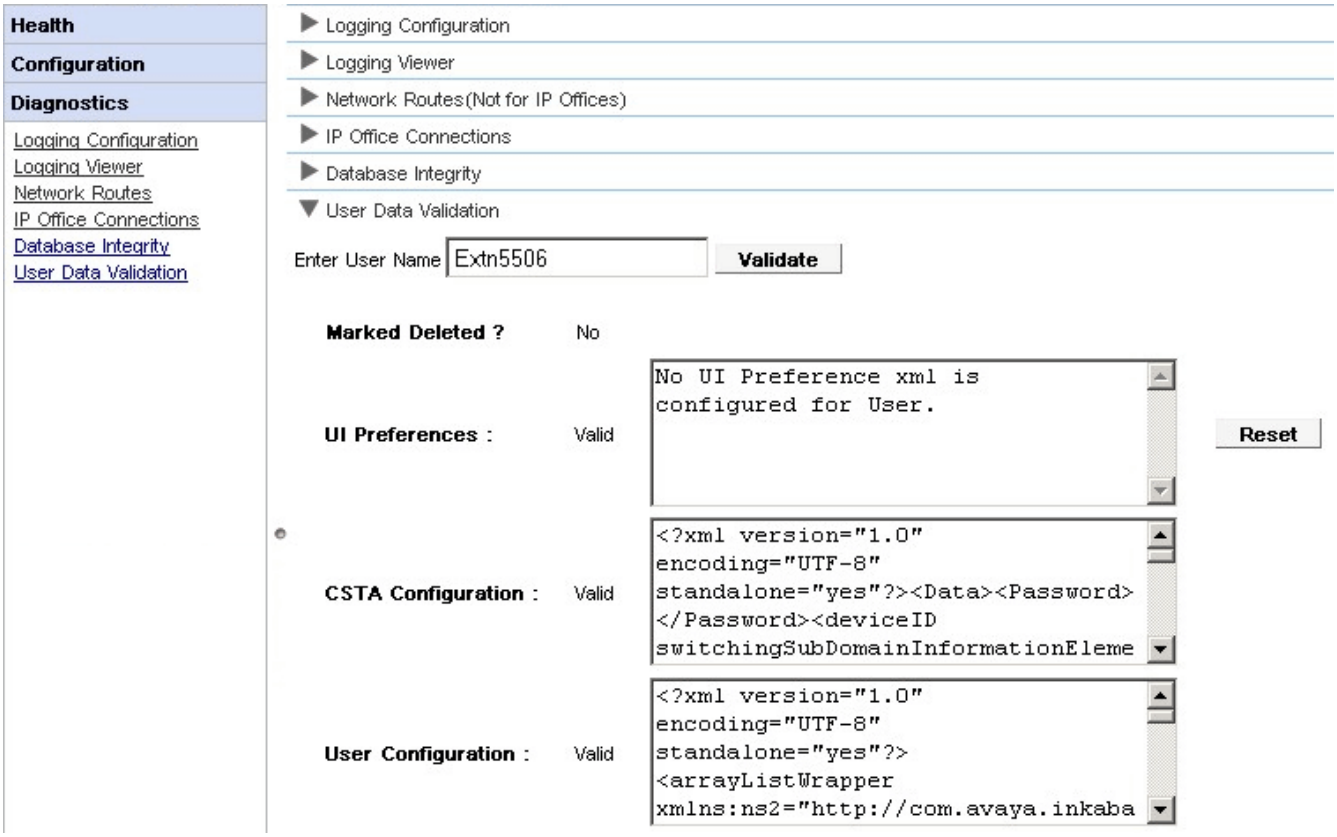
2.4.5 Intégrité de la base de données

Ce menu permet de vérifier la structure de la base de données. Il renvoie **Succès** si les tables et champs de la base de données se présentent comme il convient pour la version de one-X Portal for IP Office en question. Il ne vérifie pas les données figurant dans les champs. S'il renvoie **Échec**, consultez la section Dépannage 93 pour en savoir plus sur les problèmes connus et la façon de les résoudre.



2.4.6 Validation des données utilisateur

L'administrateur et le groupe d'assistance Avaya Backbone peuvent identifier les causes potentielles de l'échec de connexion ou de l'altération des données d'un utilisateur et peuvent réinitialiser les données altérées à l'aide de la fonction de diagnostic de one-X Portal for IP Office.

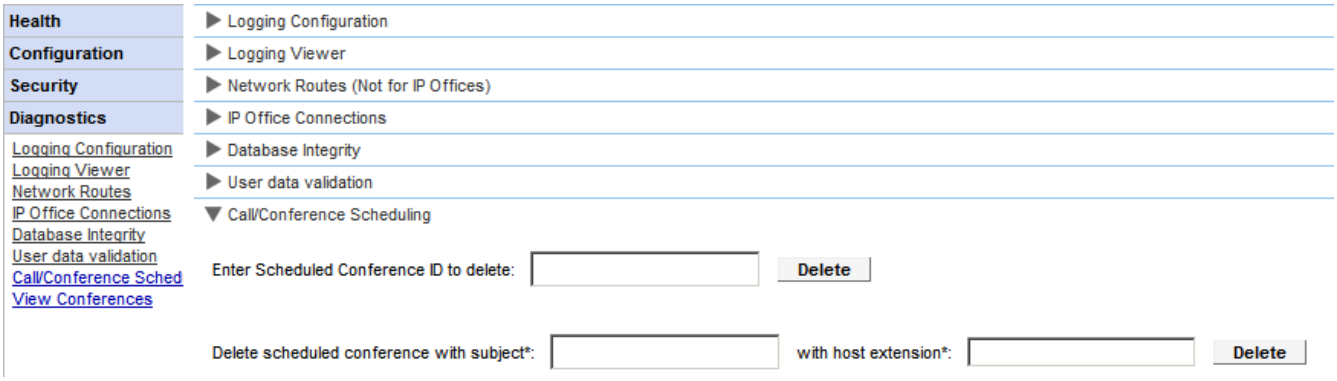


Pour afficher la validation des données utilisateur :

1. Dans l'interface administrateur de one-X Portal for IP Office, cliquez sur **Diagnostic**.
2. Sélectionnez **Validation des données utilisateur** pour afficher le formulaire correspondant à droite.
3. **Saisissez le nom** de l'utilisateur dont les données doivent être vérifiées. Ce champ possède une fonction de saisie automatique sous forme de menu déroulant.
4. Cliquez sur **Valider**. Le système valide certains champs des données de l'utilisateur dans la base de données et affiche les résultats. Champs validés :
   - **Marqué comme supprimé ? :** si l'enregistrement de l'utilisateur est marqué comme supprimé ou non.
   - **Préférences de l'interface utilisateur :** si les données de préférences de l'interface utilisateur, ainsi que les fichiers XML correspondants, sont valides ou non. Un bouton **Réinitialiser** permet de réinitialiser les données si elles sont corrompues. Les préférences de l'interface utilisateur sont restaurées et remplacées par les paramètres d'usine par défaut. L'utilisateur doit se reconnecter afin d'accéder à one-X Portal for IP Office.
   - **Configuration CSTA :** Si les données de configuration CSTA, ainsi que les fichiers XML correspondants, sont valides ou non.
   - **Configuration de l'utilisateur :** Si les données de configuration de l'utilisateur, ainsi que les fichiers XML correspondants, sont valides ou non.

2.4.7 Programmation d'appel/de conférence

Vous pouvez supprimer une conférence programmée. S'il s'agit d'une conférence régulière, toutes les occurrences qui lui sont associées seront supprimées également.

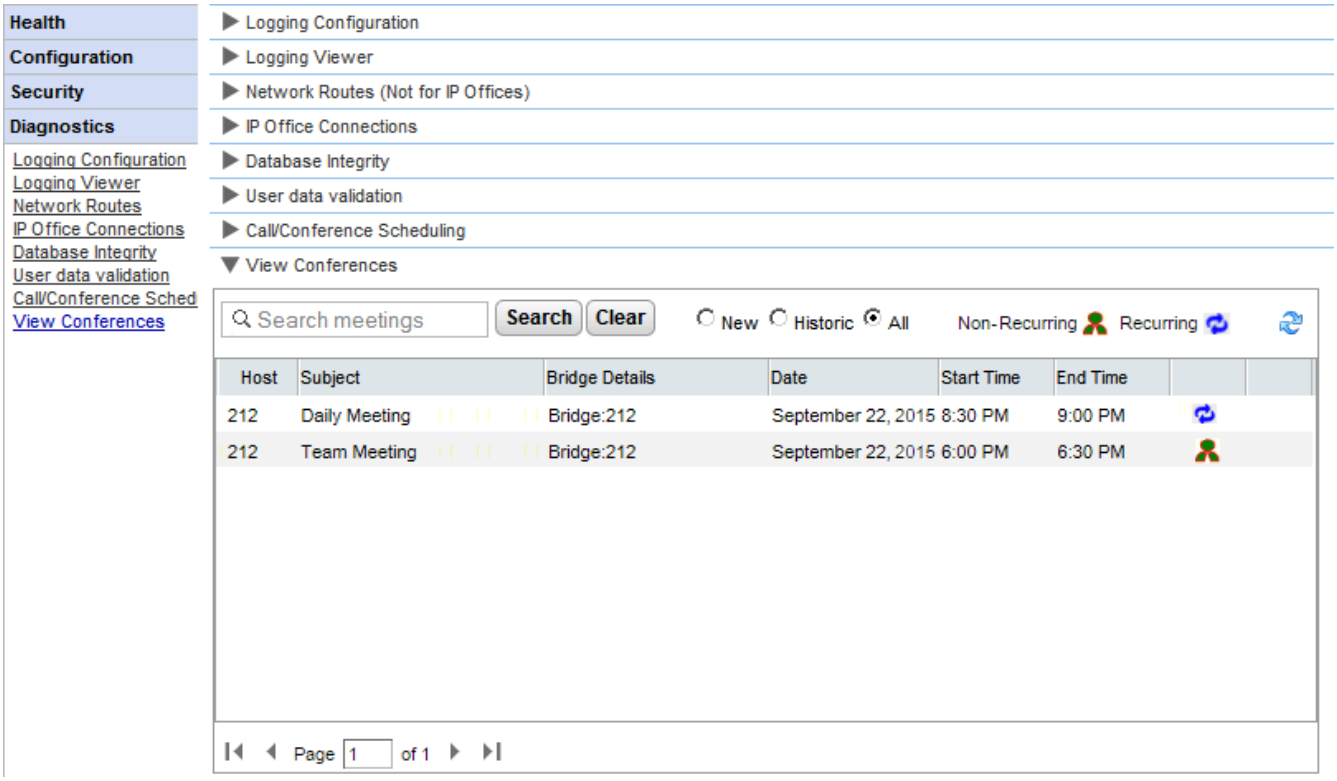


Pour supprimer une conférence ou plusieurs conférences programmées :

1. Cliquez sur **Diagnostics**, puis sélectionnez **Programmation des appels/conférences**.
2. Saisissez l'extension de l'hôte et un objet. Si vous n'indiquez pas d'objet, toutes les conférences programmées par l'hôte seront supprimées.
3. Cliquez sur **Supprimer**.

2.4.8 Affichage des conférences

Ce menu affiche le calendrier des conférences planifiées, sous une forme semblable à celui que les utilisateurs individuels de one-X Portal for IP Office peuvent afficher et utiliser. Il est toutefois différent, dans la mesure où il affiche les conférences planifiées pour tous les utilisateurs. Vous pouvez utiliser ce menu pour supprimer une conférence planifiée ou pour modifier les détails des conférences futures.



2.4.9 Générer un fichier de vidage mémoire

Afin de détecter les problèmes, Avaya peut demander un vidage de mémoire. Ce menu crée un fichier journal de vidage mémoire pour l'état actuel de fonctionnement du serveur. Le fichier est nommé en fonction de la date et de l'heure, avec l'extension **.hprof**.

Sur les serveurs basés sur Linux, tous les fichiers de vidage mémoire existants sont inclus dans les fichiers journaux téléchargeables à partir des menus de contrôle Web / d'affichage de la plate-forme du serveur (**Journaux | Télécharger**).

2.4.10 Générer un thread dump

Afin de détecter les problèmes, Avaya peut demander un thread dump. Ce menu crée un fichier journal de thread dump pour l'état actuel de fonctionnement du serveur. Le fichier s'intitule ***onex_thread_dump*** suivi de la date, de l'heure et de l'extension **.log**.

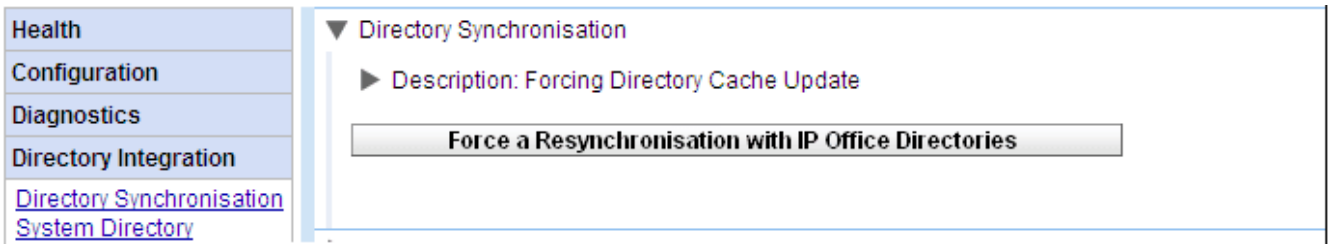
Sur les serveurs basés sur Linux, tous les fichiers de vidage mémoire existants sont inclus dans les fichiers journaux téléchargeables à partir des menus de contrôle Web / d'affichage de la plate-forme du serveur (**Journaux | Télécharger**).

2.5 Intégration des répertoires

Cette section vous permet d'afficher et de vérifier l'intégration des serveurs avec les répertoires qu'ils utilisent.

2.5.1 Synchronisation des répertoires

Dans des conditions normales de fonctionnement, le serveur one-X Portal for IP Office met à jour les enregistrements toutes les 300 secondes environ. Cependant, ce menu peut être utilisé pour forcer une mise à jour du répertoire système et des utilisateurs de IP Office.



- **Forcer une nouvelle synchronisation avec les répertoires IP Office**
  Demande une mise à jour des entrées des répertoires système stockés dans les configurations des systèmes IP Office. Vous pouvez également afficher et vérifier les entrées du **répertoire système** via l'option **Intégration des répertoires | Répertoire système** 45.

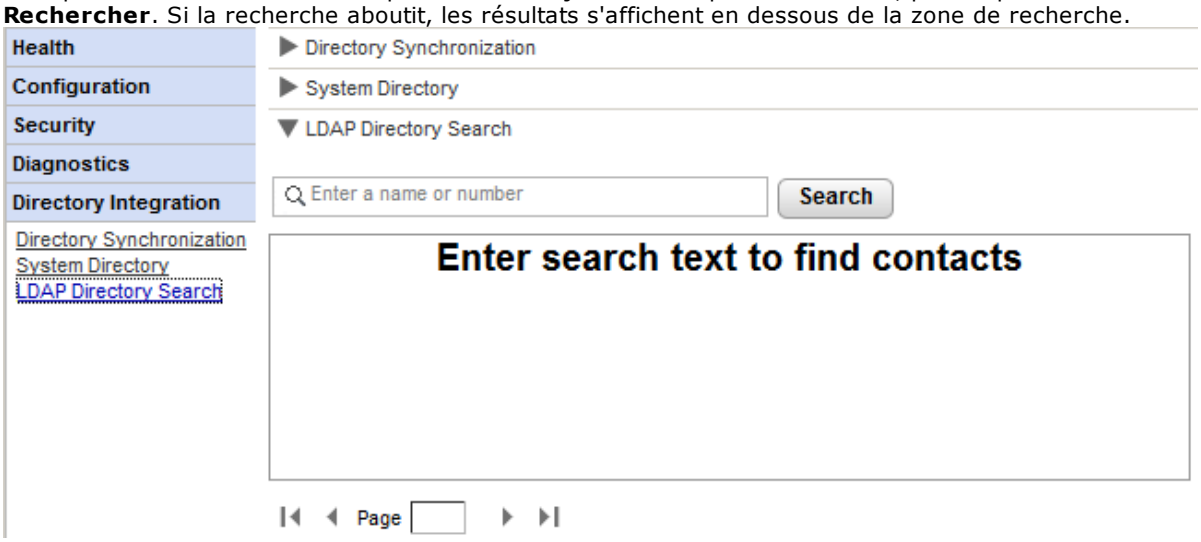
2.5.2 Recherche dans le répertoire LDAP

Cette option permet d'effectuer des recherches dans le répertoire externe de la même manière que les utilisateurs de one-X Portal for IP Office. Cela vous permet de vérifier que le fournisseur LDAP 68 est opérationnel.

Pour effectuer une recherche dans le répertoire LDAP :

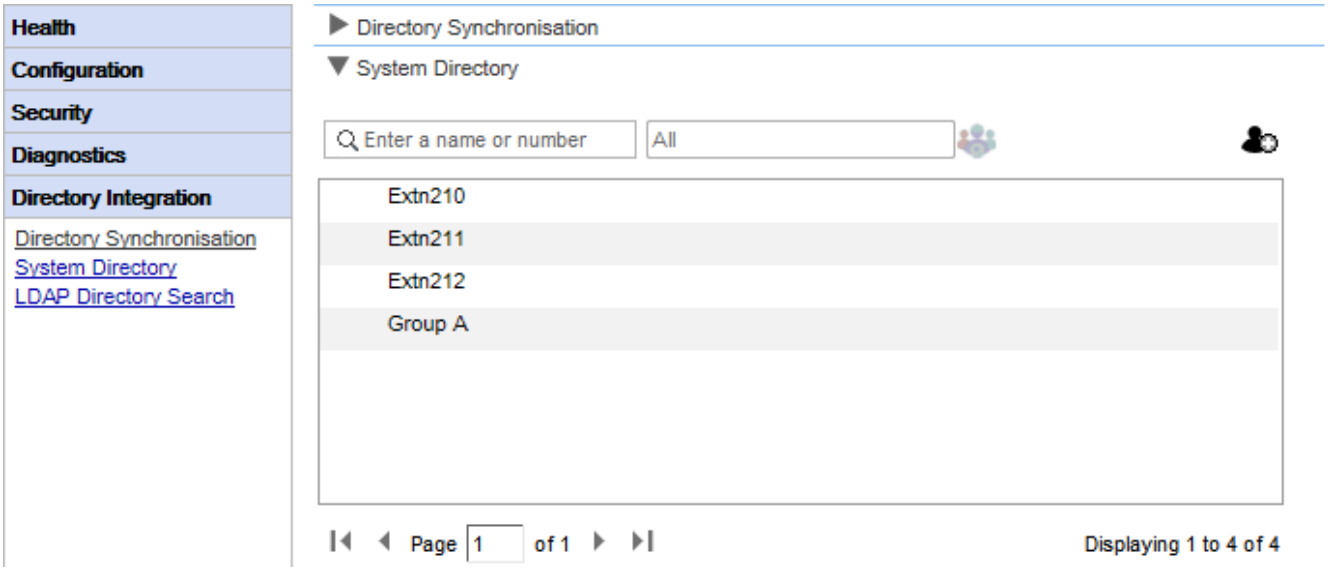
1. Sélectionnez **Intégration des répertoires**.
2. Sélectionnez **Recherche dans le répertoire LDAP**.

3. Indiquez un nom ou un numéro qui se trouve déjà dans le répertoire externe, puis cliquez sur **Rechercher**. Si la recherche aboutit, les résultats s'affichent en dessous de la zone de recherche.



2.5.3 Annuaire système

Cette option affiche le répertoire système, tel qu'il se présente aux utilisateurs de one-X Portal for IP Office. Vous pouvez effectuer des recherches dans le répertoire de la même manière que si vous utilisiez le client one-X Portal for IP Office.



Ce menu permet de vérifier que le répertoire se présente comme il convient, avec les utilisateurs, les groupes et les entrées de répertoire provenant de chaque système IP Office pris en charge.

- **Remarque :** Le système n'affiche pas les groupes définis sur *« Hors répertoire »* dans la configuration du système téléphonique.

Le serveur one-X Portal for IP Office met à jour les enregistrements des répertoires système et personnels toutes les 300 secondes environ. Vous pouvez effectuer une mise à jour manuelle à l'aide de l'option **Synchronisation des répertoires** 43.

- one-X Portal for IP Office indique l'état actuel de certains contacts du répertoire au moyen de différentes icônes. Pour les contacts possédant plusieurs numéros de téléphone, l'état repose sur le numéro professionnel.

État	Icône	Description
Disponible		État normal d'un utilisateur indiquant que son poste professionnel est libre.
Occupé		État normal d'un utilisateur indiquant qu'un appel est en cours sur son extension professionnelle.
Ne pas déranger		L'utilisateur a sélectionné l'option **Ne pas déranger**. Les appels vers son téléphone sont redirigés vers la messagerie vocale, si elle est activée, ou obtiennent une tonalité d'occupation, sauf si l'appelant figure dans la liste **Exceptions à Ne pas déranger** de l'utilisateur.
Déconnecté		L'utilisateur s'est déconnecté de son téléphone. Ses appels sont normalement redirigés vers la messagerie vocale, si elle est disponible.
Autre		Cette icône est utilisée quand l'état n'est pas connu ou ne peut pas être connu. C'est par exemple le cas des numéros externes.
En sonnerie		Cette icône est utilisée pour un contact interne qui sonne actuellement.

Ajout et modification des contacts du portail

Vous pouvez utiliser l'icône  pour ajouter un nouveau contact au répertoire système. Notez que les contacts ajoutés de cette manière sont uniquement stockés par one-X Portal for IP Office et que les utilisateurs peuvent uniquement y accéder via one-X Portal for IP Office. Le cas échéant, il est possible d'ajouter plusieurs numéros de téléphone et adresses électroniques à ces contacts.

Pour supprimer un contact ajouté de cette manière, cliquez dessus puis sélectionnez l'icône Supprimer  .

2.6 Configuration des gadgets

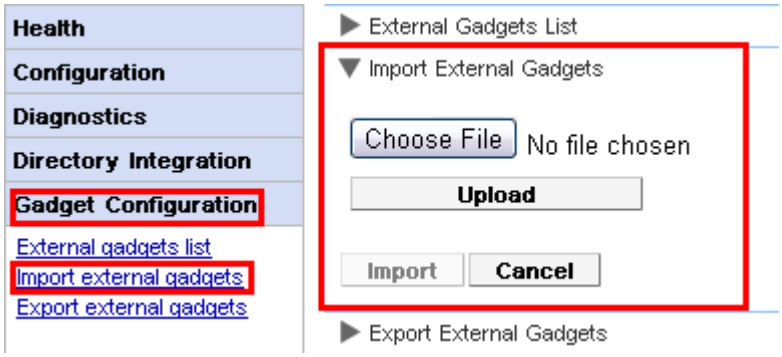
En tant qu'administrateur de one-X Portal for IP Office, vous pouvez configurer une liste de gadgets externes dans le système. Vous pouvez activer, modifier et supprimer les gadgets que l'utilisateur de one-X Portal for IP Office a la possibilité d'ajouter. L'utilisateur de one-X Portal for IP Office ne peut ajouter que les gadgets externes que l'administrateur active.

2.6.1 Liste des gadgets externes

Tous les gadgets externes du système sont répertoriés dans la **Liste de gadgets externes**. Par défaut, aucun gadget externe n'est configuré dans one-X Portal for IP Office. En tant qu'administrateur, vous pouvez ajouter un gadget externe 64 ou importer des gadgets externes 61 pour l'utilisateur.

2.6.2 Importation de gadgets

Vous pouvez importer des gadgets externes sous forme de fichier XML. Ces gadgets sont ensuite disponibles pour que les utilisateurs puissent les sélectionner. Voir Importation de gadgets 61.



Pour importer un fichier de gadget :

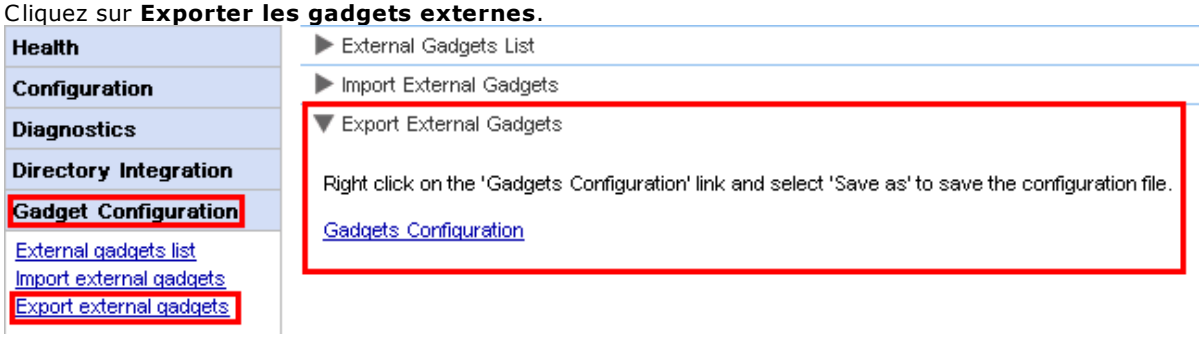
1. Cliquez sur **Configuration de gadget** et sélectionnez **Importer les gadgets externes**.
2. Cliquez sur **Choisir un fichier** pour rechercher le fichier de configuration.
3. Cliquez sur **Charger**. Le système télécharge le fichier XML sur one-X Portal for IP Office.
4. Cliquez sur **Importer** pour ajouter le gadget tiers à la *liste des gadgets*.
5. À la prochaine connexion de l'utilisateur à one-X Portal for IP Office, le gadget tiers est disponible pour que l'utilisateur l'ajoute à son portail.

2.6.3 Exportation de gadgets

L'ensemble de gadgets externes existant de one-X Portal for IP Office peut être exporté en tant que fichier de configuration. Le fichier de configuration est au format XML. Ce fichier de configuration contient des informations sur les paramètres des gadgets. Vous pouvez ajouter cet ensemble de gadgets à l'application one-X Portal for IP Office d'un autre utilisateur en [important](#) le fichier de configuration enregistré.

Pour exporter un gadget tiers :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Exporter les gadgets externes**.



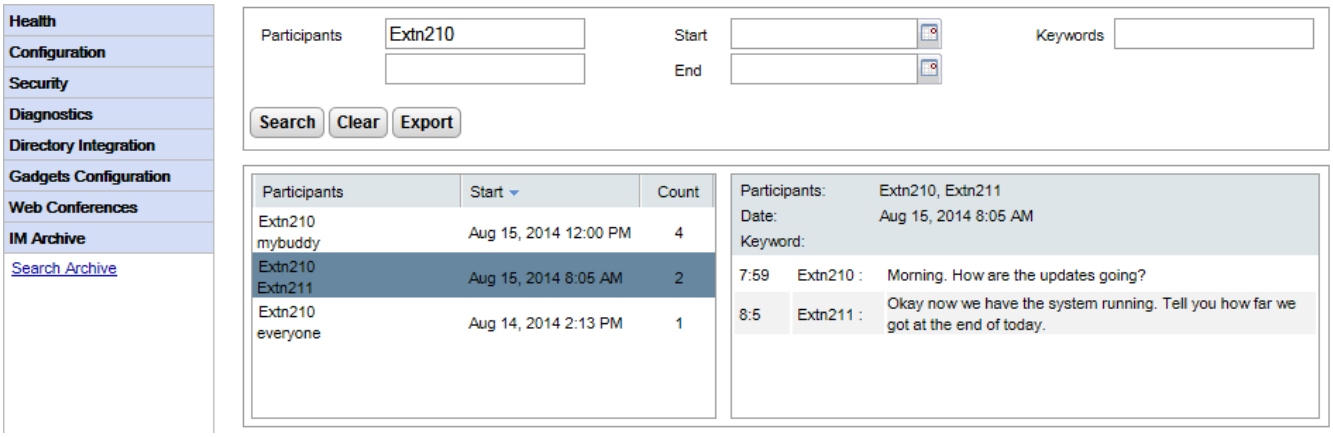
3. Cliquez avec le bouton droit de la souris sur le lien **Configuration de gadget**.
4. Sélectionnez ***Enregistrer sous*** pour enregistrer le fichier de configuration.

2.7 Archives MI

En tant qu'administrateur de one-X Portal for IP Office, vous pouvez rechercher les conversations par MI de tous les utilisateurs. Voir Activation/désactivation de l'archivage MI 76.

2.7.1 Rechercher dans les archives

Vous pouvez rechercher des conversations sur les messageries instantanées ayant eu lieu entre les utilisateurs et depuis le système vers un utilisateur.. Tous les champs du volet de recherche sont facultatifs. Le nombre de jours pendant lequel le serveur conserve une conversation MI dans les archives est défini grâce au paramètre **Nombre de jours d'archivage MI** 77.



Pour effectuer une recherche dans les archives MI :

1. Dans le volet de gauche, cliquez sur **Archives MI**.
2. Cliquez sur **Rechercher dans les archives**.
3. Saisissez les critères de recherche, puis cliquez sur Rechercher.

Champ	Description
Participants	Saisissez le nom du participant à la conversation par MI.
Mots clés	Tapez les mots clés dans la conversation MI.
Démarrer	Sélectionnez la date à partir de laquelle vous voulez rechercher les conversations. Si vous ne sélectionnez pas de date, le système affiche les conversations à partir de la plus ancienne conservée par le système.
Fin	Sélectionnez la date des dernières conversations que vous voulez consulter. Si vous ne sélectionnez pas de date, le système affiche les résultats jusqu'à la toute dernière conversation.

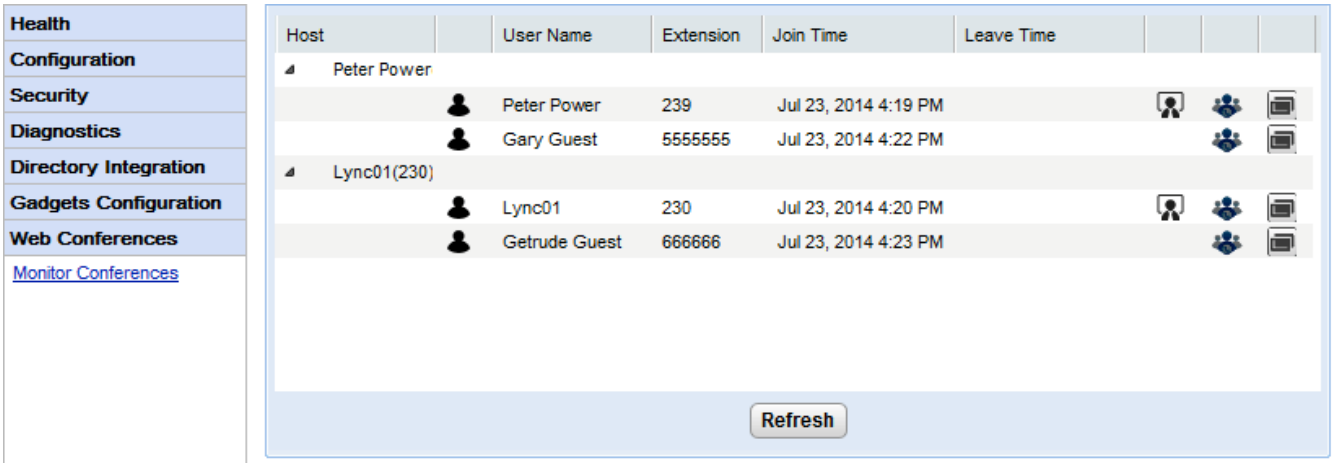
4. Cliquez sur la conversation que vous voulez ouvrir. Le système ouvre la conversation.

2.8 Conférences Web

Sur les systèmes de portail sous IP Office Server Edition et IP Office Application Server, le serveur one-X Portal for IP Office peut afficher les détails des conférences audio en cours.

2.8.1 Contrôler les conférences

Ce menu permet d'afficher le détail des conférences de collaboration web hébergées par le serveur. Il répertorie les membres participant aux conférences et indique l'heure de leur dernière connexion, ainsi que l'objet de leur participation (présentateurs, membres des conférences audio, membres des conférences web). Ce menu n'est pas pris en charge sur le serveur Unified Communications Module.



Pour afficher les conférences en cours :

1. Sélectionnez **Conférences Web**, puis **Contrôler les conférences**.
2. Les conférences web en cours figurent dans la liste.
3. Cliquez sur **Hôte** pour agrandir la fenêtre de la conférence et afficher des informations sur les participants.

2.9 Aide et assistance technique

Aide | Aide

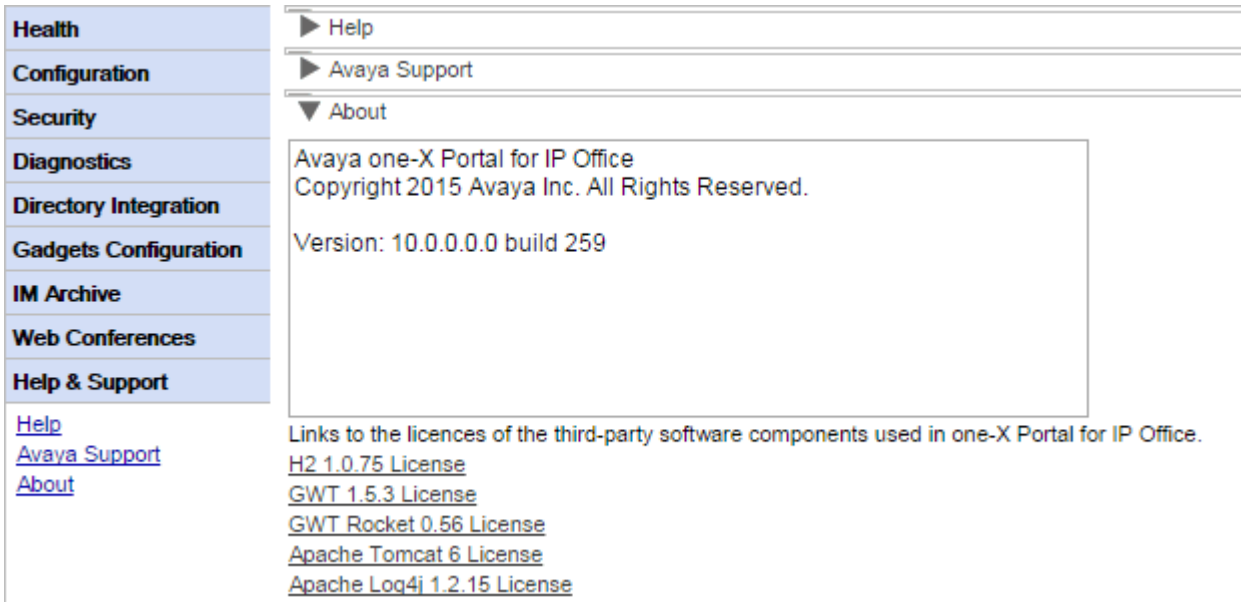
Fournit des liens d'aide vers one-X Portal for IP Office destinée aux utilisateurs et vers le présent document.

Aide | Assistance technique Avaya

Charge un lien vers le site Web d'assistance technique Avaya (http://support.avaya.com).

Aide | À propos de

Affiche les informations de base sur la version du logiciel one-X Portal for IP Office installé.



Chapitre 3.
Tâches de maintenance

3. Tâches de maintenance

3.1 Redémarrage du service

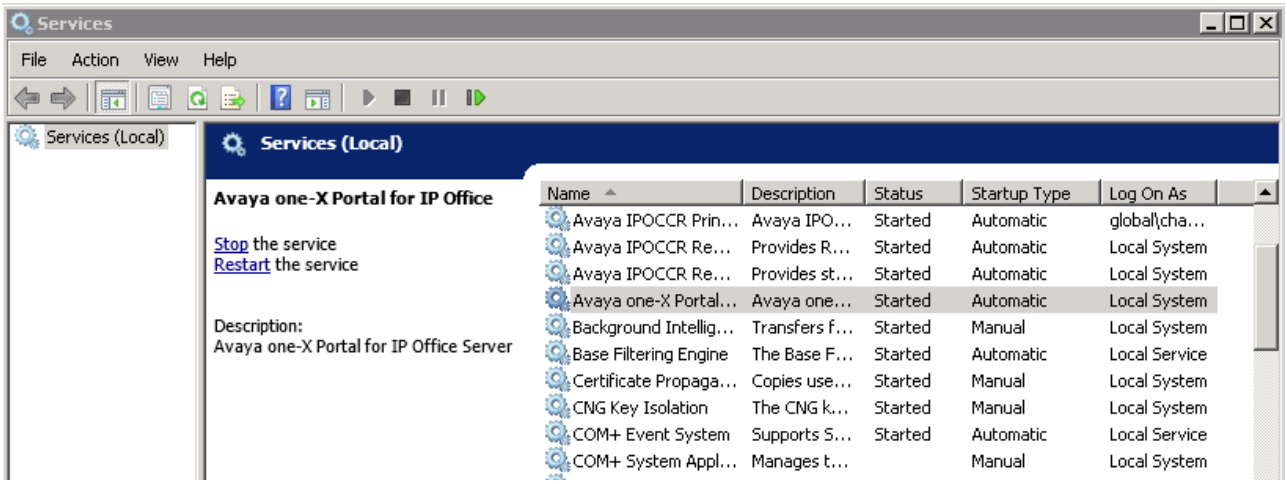
Vous pouvez arrêter et démarrer le service one-X Portal for IP Office de différentes manières.

À partir des menus d'administration

Cliquez sur l'icône en haut des menus d'administration pour redémarrer le portail. Notez que cette icône s'affiche automatiquement si vous effectuez une modification qui nécessite un redémarrage.

Serveur sous Windows

L'application one-X Portal for IP Office s'installe sous forme d'un service intitulé one-X Portal Avaya. Vous pouvez la démarrer et l'arrêter à partir du Panneau de configuration Services standard de Windows.



Après le démarrage ou le redémarrage du service, le service one-X Portal Avaya indique au bout de quelques secondes qu'il est prêt. Notez toutefois que cela pourrait prendre jusqu'à 15 minutes pour que l'application ne soit entièrement opérationnelle. Vous pouvez par exemple utiliser Windows Task Manager pour suivre la progression du processus. En général, lors du démarrage de one-X Portal for IP Office, la valeur **Util. du fichier** augmente progressivement jusqu'à environ 2.3 Go avant que one-X Portal for IP Office ne démarre.

- **Pas de service !**
  Si le service n'est pas présent, cela est probablement dû à un conflit de port ou à un problème de Java. Reportez-vous à la section Dépannage 93.

Serveur sous Linux

1. Dans les menus de gestion web, sélectionnez **Solution**.
2. Cliquez sur l'icône et sélectionnez **Vue de la plate-forme**.
3. Dans la vue de la plateforme, l'état du service one-X Portal est affiché dans l'onglet **Système**. Pour arrêter le service, cliquez sur **Arrêter** ou **Forcer à arrêter**. Pour lancer le service, cliquez sur **Démarrer**.

3.2 Configuration du journal des appels

Le journal des appels de l'utilisateur affiché par one-X Portal for IP Office est stocké sur le système téléphonique dans votre configuration utilisateur. 30 enregistrements maximum sont stockés et les nouveaux enregistrements remplacent les plus anciens lorsque la limite est atteinte. Cependant, pour les appels répétés ou provenant du même numéro, l'enregistrement existant est mis à jour et le décompte du nombre d'appels augmente.

Pour les appels entrants, par défaut, uniquement les appels personnels (hors appels collectifs) à l'utilisateur ayant été répondus par l'utilisateur ou non répondus sont compris dans le journal des appels.

- **Appels manqués**
  Les appels que l'utilisateur ne prend pas mais qui sont redirigés vers la messagerie vocale ou un autre poste sont normalement classés dans la liste des appels manqués. Pour activer la journalisation des appels manqués, le paramètre système **Journaliser les appels manqués répondus sur couverture** (**Système | Téléphonie | Journal des appels**) doit être activé dans la configuration du système téléphonique IP Office.
- **Appels collectifs manqués**
  Par défaut, seuls les appels collectifs auxquels l'utilisateur répond sont journalisés. Pour activer la journalisation des appels collectifs manqués, le paramètre système **Journaliser les appels collectifs manqués** doit également être activé dans la configuration du système téléphonique IP Office. L'utilisateur doit également être configuré dans les systèmes téléphoniques avec les groupes pour lesquels le journal inclut les appels manqués (**Utilisateur | Téléphonie | Journal des appels**).
- **Suppression automatique**
  Les archives des anciens appels sont automatiquement supprimées lorsque la capacité maximale de journalisation a été atteinte et qu'un nouvel appel doit être ajouté. Vous pouvez en outre configurer le système téléphonique de façon à ce qu'il supprime les entrées de journal après une période donnée. Cliquez sur **Supprimer les entrées après** (**Utilisateur | Téléphonie | Journal des appels**).

Historique des conversations téléphoniques

Les utilisateurs employant un téléphone de série 1400, 1600, 9500 ou 9600 avec un bouton **Journal d'appels** ou **Historique**, ou un téléphone de série M ou T, par défaut le même journal d'appels que celui qui figure dans le portail est affiché sur le téléphone. Vous pouvez ensuite utiliser et modifier le journal des appels sur le téléphone ou dans one-X Portal for IP Office. Les deux versions changent en parallèle.

Les utilisateurs employant un autre type de téléphone possédant un journal d'appels, il s'agira d'un journal en mémoire dans le téléphone. Par conséquent, il ne correspondra pas nécessairement au journal des appels indiqué dans one-X Portal for IP Office. Par exemple, les appels effectués via one-X Portal for IP Office n'apparaîtront pas dans le journal d'appels du téléphone et vice versa.

Dans les deux cas, le journal des appels one-X ne peut afficher que 255 entrées.

3.3 Commutateur IP Office

3.3.1 Ajout d'un système IP Office supplémentaire

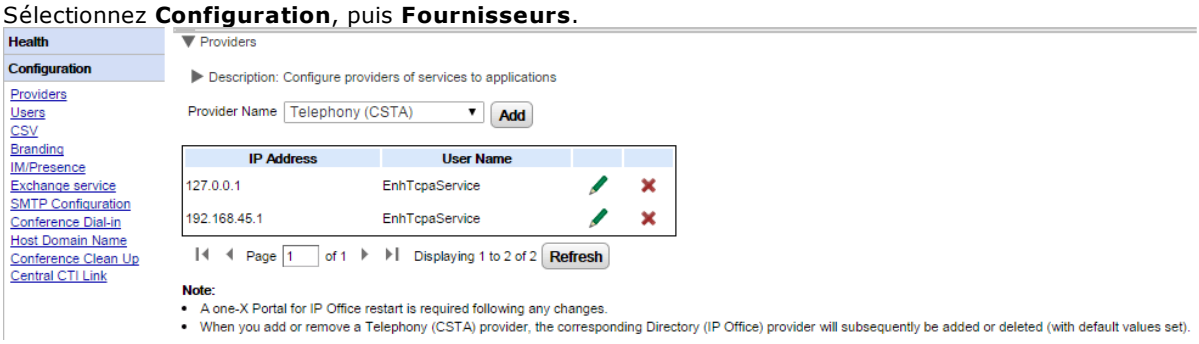
Pour ajouter un système IP Office supplémentaire à un réseau de petit groupe, il faut attribuer son adresse IP aux fournisseurs Téléphonie (CSTA) et Annuaire (IP Office).

- **Mise en service automatique/Mode CTI centralisé** 33
  Lorsqu'un serveur de portail sous Linux prend en charge un réseau IP Office Server Edition, le système IP Office principal peut lui envoyer des informations sur les autres systèmes IP Office du réseau et sur le serveur de messagerie vocale. Il ajoute ou supprime alors automatiquement les fournisseurs appropriés pour ces autres systèmes. À l'aide du **paramètre Liaison CTI centrale**, disponible par défaut pour les nouvelles installations. Une fois ce paramètre activé, la configuration manuelle des fournisseurs pour les systèmes IP Office supplémentaires n'est plus nécessaire. En mode CTI centralisé :
  - Si la résilience n'est pas utilisée, le serveur nécessite un seul fournisseur DMSL pour le système IP Office principal.
  - Si la résilience est utilisée, le serveur a uniquement besoin d'un fournisseur DSML pour les systèmes IP Office principal et secondaire.
  - Le serveur nécessite un seul fournisseur CSTA pour le système IP Office principal, sauf si vous utilisez la résilience de portail, auquel cas il doit également y avoir un fournisseur CSTA pour le système IP Office secondaire.

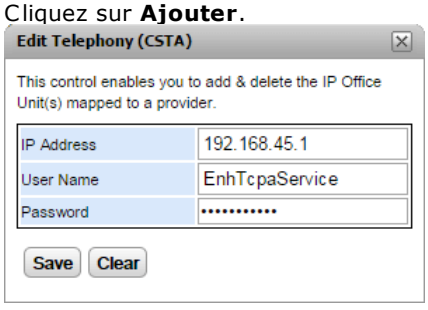
Pour ajouter un autre système IP Office :

- **Attention**
  Pour ce processus, vous devez redémarrer le service de portail 52 pour que les modifications soient prises en compte. Pendant le redémarrage, il est possible que les utilisateurs ne puissent accéder au portail pendant une durée pouvant atteindre 15 minutes.

1. Avant d'ajouter un autre système IP Office à la configuration one-X Portal for IP Office :
   - Vérifiez que le système IP Office a été configuré avec les paramètres de sécurité nécessaires au fonctionnement de one-X Portal for IP Office.
   - Vérifiez que le système IP Office possède les licences nécessaires pour utiliser one-X Portal for IP Office.
   - Vérifiez qu'au moins un utilisateur du système IP Office a été activé pour utiliser one-X Portal for IP Office.
2. Connectez-vous 9 aux menus d'administration.
3. Vérifiez que le serveur one-X Portal for IP Office peut voir le système IP Office.
   a. Sélectionnez **Diagnostics**, puis **Connexions IP Office**.
   b. Saisissez l'**adresse IP** du système IP Office cible, puis cliquez sur **Vérifier**.
   c. Si le système IP Office est accessible, les résultats incluent ses informations de base.
4. Sélectionnez **Configuration**, puis **Fournisseurs**.



5. Cliquez sur **Ajouter**.



6. Saisissez l'**adresse IP** du nouveau système IP Office.

7. Saisissez le **nom d'utilisateur** et le **mot de passe** de l'utilisateur de sécurité TCPA configuré dans le système IP Office.
8. Cliquez sur **Enregistrer**.
9. Redémarrez le service one-X Portal Avaya 52. Une fois que le service a redémarré dans son intégralité, connectez-vous de nouveau aux menus d'administration.
10. Sélectionnez **Santé**, puis **État des composants**.
11. Cliquez sur **Obtenir tout**. Les nouveaux composants CSTA et DSML pour l'adresse IP du nouveau système IP Office ajouté sont à présent inclus. L'état de ces composants est normalement indiqué.
12. Sélectionnez **Intégration des répertoires**. Vérifiez que les nouveaux utilisateurs du système IP Office sont répertoriés. Si ce n'est pas le cas, sélectionnez **Synchronisation des répertoires | Forcer une nouvelle synchronisation avec les répertoires IP Office**, puis patientez 5 minutes.
13. Sélectionnez **Configuration**, puis **Utilisateurs**. Cliquez sur **Obtenir tout**. Vérifiez que les nouveaux utilisateurs du système IP Office sont répertoriés.

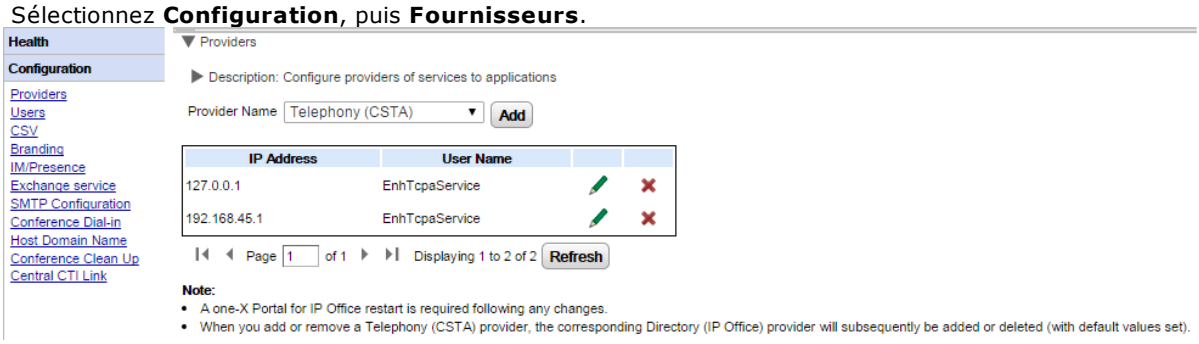
3.3.2 Modification des détails IP Office

Si les détails (adresse IP, nom d'utilisateur et mot de passe du service TCPA) d'un système IP Office attribué sont modifiés, il est nécessaire d'actualiser les paramètres IP Office dans les fournisseurs de one-X Portal for IP Office en conséquence.

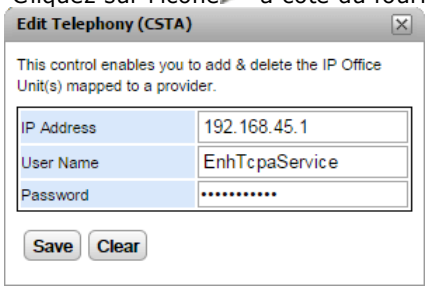
- **Attention**
  Pour ce processus, vous devez redémarrer le service de portail 52 pour que les modifications soient prises en compte. Pendant le redémarrage, il est possible que les utilisateurs ne puissent accéder au portail pendant une durée pouvant atteindre 15 minutes.

Pour modifier les informations relatives à IP Office :

1. Connectez-vous 9 aux menus d'administration.
2. Si c'est l'adresse IP du système IP Office qui a changé, vérifiez que le système IP Office est visible depuis le serveur one-X Portal for IP Office.
   a. Sélectionnez **Diagnostics**, puis **Connexions IP Office**.
   b. Saisissez l'**adresse IP** du système IP Office cible, puis cliquez sur **Vérifier**.
   c. Si le système IP Office est accessible, les résultats incluent ses informations de base.
3. Sélectionnez **Configuration**, puis **Fournisseurs**.



4. Cliquez sur l'icône à côté du fournisseur CSTA existant auquel le système IP Office a été attribué.



5. Modifiez les détails affichés pour qu'ils correspondent aux nouveaux paramètres du système IP Office puis cliquez sur **Enregistrer**.
6. Redémarrez le service de portail 52.

3.3.3 Résilience

Dans IP Office version 10 et ultérieures, le service de portail est également installé par défaut sur le serveur secondaire IP Office Server Edition. Cela permet au serveur d'agir comme serveur de portail pour les utilisateurs lorsque le serveur principal n'est pas disponible, quelle qu'en soit la raison.

- La résilience du portail est prise en charge sous le mode IP Office Server Edition Select. Il est également possible de configurer la résilience de portail en utilisant un IP Office Application Server au lieu du service de portail du serveur principal ou secondaire.
    - Sur les systèmes existants en mode de non sélection basculés vers le mode IP Office Server Edition Select, un redémarrage des services du portail peut être requis afin que les paramètres de résilience soient disponibles. De même, il peut être nécessaire de redémarrer les service de portail après la première configuration de la résilience de portail lors de la configuration du système IP Office.
- La résilience est uniquement prise en charge entre des serveurs principal et secondaire exécutant la même version du logiciel de portail.
- Lorsque les serveurs fonctionnent normalement, c'est-à-dire lorsqu'ils sont en cours d'utilisation et connectés, les modifications effectuées par les utilisateurs ou l'administrateur sur le serveur principal sont automatiquement synchronisées sur le serveur secondaire. Toutefois, pendant la résilience, les modifications effectuées sur l'un des serveurs ne sont pas synchronisées et peuvent être perdues lors que les serveurs fonctionnent à nouveau normalement.
    - Les conférences planifiées font actuellement partie des exceptions à la règle ci-dessus. Les conférences planifiées sur le serveur principal n'ont pas lieu lors du fonctionnement en mode de reprise. Les conférences planifiées sur le serveur secondaire sont perdues lorsque la restauration a lieu.
- Dans l'affichage de la plate-forme (panneau de contrôle Web) de chaque serveur :
    - le serveur de portail actif est 'Disponible' (une icône verte).
    - le serveur de portail actif est 'En cours de démarrage' (une icône ambrée).
- Les applications de portail client one-X Portal Call Assistant ne sont pas automatiquement redirigées. L'utilisateur doit saisir l'adresse du serveur secondaire pour se connecter.

Lorsque la résilience de portail est configurée :

- **En cas de défaillance du portail du serveur principal**
  Si le service de portail du serveur principal s'interrompt pour une quelconque raison, le service de portail du serveur secondaire devient automatiquement disponible.
    - Les utilisateurs qui étaient connectés au portail du serveur principal peuvent de nouveau se connecter au serveur secondaire.
        - Si le service principal IP Office est encore actif, les utilisateurs de ce portail sont automatiquement redirigés.
        - Si les utilisateurs n'ont pas accédé au serveur de portail secondaire précédemment, il se peut qu'ils doivent accepter le certificat de sécurité ou créer une exception qui interrompra la reconnexion automatique.
    - Il en va de même pour les utilisateurs qui étaient connectés à l'un des clients du portail tels qu'Outlook.
    - Les nouveaux utilisateurs souhaitant se connecter devront utiliser l'adresse du serveur secondaire.
- **En cas de défaillance du service IP Office sur le serveur principal :**
  Si le service du serveur IP Office principal s'interrompt pour une quelconque raison, les services de portail sont automatiquement transférés sur le serveur secondaire, tel que décrit ci-dessus.
    - Lorsque le noyau IP Office n'est pas actif, les utilisateurs qui appartiennent à ce noyau IP Office ne peuvent mettre à jour ni supprimer des contacts personnels à partir du gadget Répertoire du portail.
- **En cas de panne réseau :**
  Si la connexion réseau entre le serveur principal et le serveur secondaire s'interrompt pour une quelconque raison, les deux serveurs de portail deviennent actifs et il est possible de s'y connecter. Ici encore, les modifications apportées aux utilisateurs et à l'administration sur le serveur de portail secondaire ne sont pas copiées sur le serveur principal une fois que la connexion réseau est rétablie. C'est ce que l'on appelle le « mode autonome ».
- **En cas de rétablissement du portail du serveur principal :**
  Lorsque le service de portail du serveur principal est de nouveau disponible, le service de portail du serveur secondaire cesse de prendre en charge les connexions.
    - Les utilisateurs qui étaient connectés au portail du serveur secondaire sont automatiquement redirigés pour se connecter de nouveau sur le serveur principal.
    - Les utilisateurs qui étaient connectés à l'un des clients du portail, par exemple le plug-in Outlook, sont automatiquement connectés au serveur principal.
    - Les nouveaux utilisateurs souhaitant se connecter sont dirigés vers le serveur principal.

- **En cas de rétablissement du service IP Office sur le serveur principal :**
  Lorsque le service IP Office du serveur principal est de nouveau disponible, le serveur principal prend de nouveaux en charge le service de portail, tel que décrit ci-dessus.

Pour configurer la résilience :

1. **Activer le mode Lien CTI centralisé**
   Les deux serveurs de portail doivent être paramétrés de manière à utiliser le mode Lien CTI centralisé. Il s'agit du paramètre par défaut pour les nouvelles installations mais, pour les systèmes existants mis à niveau vers IP Office version 10 ou supérieure, ce paramètre doit être activé manuellement.
   a. Le mode Lien CTI centralisé peut être activé via le menu **Lien CTI centralisé** 33.
   b. Si vous modifiez ce paramètre, vous devez alors redémarrer le service de portail pour que la modification prenne effet.
   c. Ce paramètre doit être activé aussi bien sur le serveur principal que sur le serveur secondaire.
2. **Activer la résilience du serveur de portail**
   Il faut que le serveur de portail principal soit configuré pour la résilience via ses menus **Configuration de la résilience** 30.
3. **Redémarrer les services de portail**
   Si des modifications sont apportées aux étapes ci-dessus.
4. **Activer de nouveau le portail sur les lignes réseau**
   Le paramètre de sauvegarde de portail doit être activé sur les lignes SCN entre les serveurs IP Office principal et secondaire.
   a. En utilisant IP Office Manager, chargez la configuration des systèmes IP Office d'IP Office Server Edition.
   b. Dans les paramètres du serveur principal, identifiez la ligne IP Office reliant le système IP Office principal au système IP Office secondaire.
   c. Dans les **Options de résilience SCN** de l'onglet **Ligne**, vérifiez que **Prise en charge de la résilience** et **Sauvegarde de mon one-X Portal** sont sélectionnés.
   d. Enregistrez les modifications apportées à la configuration.

3.4 Gadgets

3.4.1 Récupération de l'URL d'un gadget

Google fournit un éventail de gadgets que vous pouvez ajouter sur votre page Web.

Exemple : Pour récupérer l'URL d'un gadget Google :

1. Pour obtenir la liste des gadgets fournis par Google, consultez : http://www.google.com/ig/directory?synd=open
2. Sélectionnez le gadget que vous souhaitez ajouter à votre page Web.
3. Cliquez sur **Ajouter à votre page Web**.
4. Cliquez sur **Obtenir le code**. Le système affiche une chaîne similaire à celle indiquée ci-dessous. Le texte situé entre " " (guillemets) est l'URL du gadget :

```
<script src="http://www.gmodules.com/ig/ifr?
url=http://www.donalobrien.net/apps/google/currency.xml&amp;up_def_from=USD&amp;up_def_to=EUR&amp;
synd=open&amp;w=320&amp;h=170&amp;title=Currency+Converter&amp;border=%23ffffff%7C0px%
2C1px+solid+%2382CAFA%7C0px%2C2px+solid+%23BDEDFF%7C0px%2C3px+solid+%
23E0FFFF&amp;output=js"></script>
```

3.4.2 Importation de gadgets

Des gadgets tiers peuvent être ajoutés à one-X Portal for IP Office à l'aide d'un fichier XML. Vous ne pouvez pas télécharger plus de 50 gadgets à la fois. La taille du fichier ne doit pas être supérieure à 2 Mo.

Pour chaque gadget, les paramètres suivants doivent être spécifiés :

- L'URL du gadget, c'est-à-dire la source du gadget ainsi que son contenu
- Le nom du gadget qui s'affichent sur la barre de titre de ce dernier
- Les icônes de la barre d'outils du gadget. Il est conseillé de fournir les icônes de barre d'outils de tous les gadgets spécifiés dans le fichier gadgets.xml.
- Textes de la barre d'outils du gadget (infobulle et texte affichés en dessous de l'icône de la barre d'outils).

Exemple de format du fichier XML d'un gadget :


```
<GadgetsConfigurationImpl>
<gadgetRecords>
<entry>
<key>1</key>
<value>
<categorys>1</categorys>
<categorys>2</categorys>
<created>2012-08-10</created>
<defaultToolbarIcon />
<downToolbarIcon />
<deleted />
<enable>true</enable>
<external>true</external>
<height>300</height>
<id>1</id>
<localizedName><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></localizedName>
<name>Angry Birds</name>
<toolbarText><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></toolbarText>
<tooltip><?xml version="1.0" encoding="UTF-8" standalone="no"?><names><en_US>Angry
Birds</en_US><en_GB>Angry Birds</en_GB><de>Angry Birds</de><fr>Angry Birds</fr><it>Angry
Birds</it><nl>Angry Birds</nl><es>Angry Birds</es><pt_BR>Angry Birds</pt_BR><ru>Angry
Birds</ru><zh>Angry Birds</zh></names></tooltip>
<url>http://www.gmodules.com/ig/ifr?
url=http://www.forumforyou.it/google_gadget_angry_birds.xml&amp;synd=open&amp;w=820&amp;h=680&amp;title
=Angry+Birds&amp;border=%23ffffff%7C3px%2C1px+solid+%23999999&amp;output=js</url>
</value>
</entry>
</gadgetRecords>
</GadgetsConfigurationImpl>
```


Remarque : Veillez à respecter les consignes suivantes dans le fichier .xml :

1. Chaque gadget doit être placé dans l'élément <entry></entry>.
2. L'élément <key></key> doit être unique et correspondre à <id></id>. Il s'agit d'un identifiant de gadget unique utilisé en interne.
3. L'élément <value></value> doit contenir les informations sur les gadgets.
4. L'élément <categorys></categorys> indique la catégorie du gadget. Les identifiants et les codes des catégories se présentent comme suit :

Code	Catégorie
1	Tous
2	Communication
3	Outils

4	Productivité
5	Finance
6	Technologie
7	Zoho

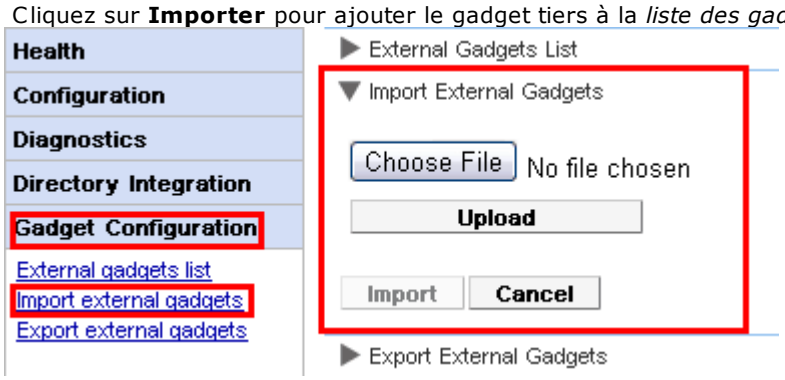
5. Détails des autres éléments :

Élement	Description
<created>	Date de création du fichier.
<defaultToolbarIcon>	Spécifie l'icône par défaut que le système affiche dans la barre d'outils lorsque vous réduisez le gadget. Le système affiche l'icône dans la barre d'outils de l'utilisateur.
<downToolbarIcon>	Spécifie l'icône par défaut que le système affiche lorsque l'utilisateur clique sur l'icône des gadgets.
<enable>	Définissez cette valeur sur « true » si vous voulez que le gadget soit visible pour l'utilisateur.
<external>	Définissez cette valeur sur « true » pour tous les gadgets externes.
<height>	Définit la hauteur du gadget en pixels.
<id>	Identifiant du gadget.
<localizedName>	Spécifie le nom localisé pour chaque langue.
<name>	Spécifie un nom unique pour le gadget.
<toolbarText>	Texte affiché par le système dans la barre d'outils du gadget.
<tooltip>	Texte affiché par le système dans l'info-bulle du gadget.
<url>	URL du gadget. Pour de plus amples informations, consultez la section Récupération de l'URL d'un gadget externe - Exemple 60

Remarque : des messages d'erreur appropriés s'affichent si le fichier de configuration ne prend en charge aucun des critères ci-dessus.

Pour importer un fichier de gadget :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Importer les gadgets externes**.
3. Cliquez sur **Choisir un fichier** pour rechercher le fichier de configuration.
4. Cliquez sur **Télécharger**. Le système télécharge le fichier XML sur one-X Portal for IP Office.
5. Cliquez sur **Importer** pour ajouter le gadget tiers à la *liste des gadgets*.



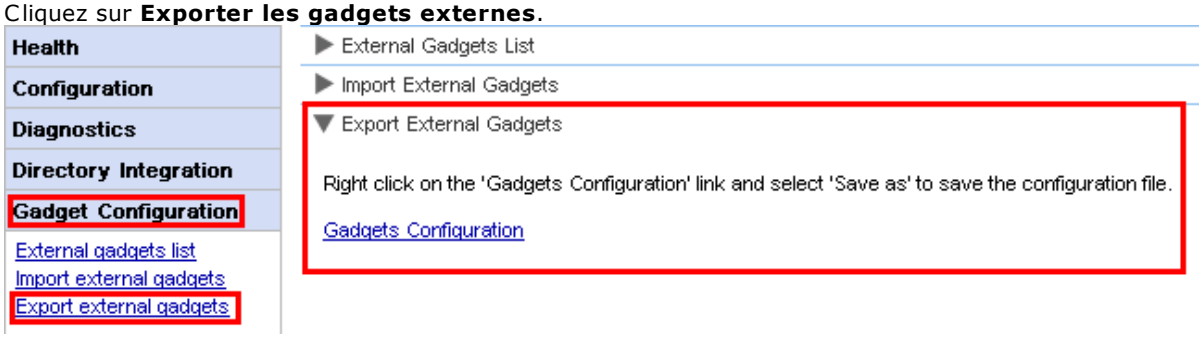
6. À la prochaine connexion de l'utilisateur à one-X Portal for IP Office, le gadget tiers est disponible pour que l'utilisateur l'ajoute à son portail.

3.4.3 Exportation de gadgets

L'ensemble de gadgets externes existant de one-X Portal for IP Office peut être exporté en tant que fichier de configuration. Le fichier de configuration est au format XML. Ce fichier de configuration contient des informations sur les paramètres des gadgets. Vous pouvez ajouter cet ensemble de gadgets à l'application one-X Portal for IP Office d'un autre utilisateur en [important](#) le fichier de configuration enregistré.

Pour exporter un gadget tiers :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Exporter les gadgets externes**.



3. Cliquez avec le bouton droit de la souris sur le lien **Configuration de gadget**.
4. Sélectionnez ***Enregistrer sous*** pour enregistrer le fichier de configuration.

3.4.4 Ajout d'un gadget externe

Pour ajouter un seul gadget, vous avez besoin de son URL. Pour obtenir davantage d'informations sur la façon d'obtenir l'URL du gadget, consultez Récupération de l'URL d'un gadget externe - Exemple 60.

Pour ajouter un gadget externe :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Liste des gadgets externes**.
3. Cliquez sur **Ajouter**. Le système affiche la boîte de dialogue **Ajouter un gadget**.
4. Ajoutez les informations relatives au gadget (voir ci-dessous) puis cliquez sur **Enregistrer**. Le système met à jour le gadget externe que vous venez d'ajouter dans la base de données one-X Portal for IP Office.

Champs du gadget

Nom du champ	Description
Nom du gadget	Le système affiche le nom que vous avez indiqué dans ce champ sur la barre de titre du gadget. Assurez-vous que le nom du gadget ne dépasse pas 50 caractères.
URL du gadget	Contient l'URL du gadget. L'URL que vous indiquez doit se conformer aux spécifications standard pour les URL figurant sur http://www.w3.org/Addressing/URL/url-spec.txt. Le système utilise l'URL que vous avez indiquée pour afficher le gadget.
Nom de gadget localisé	Le système affiche le nom localisé que vous avez indiqué dans ce champ sur la barre de titre du gadget. Le système n'affiche le nom localisé que si l'utilisateur de one-X Portal for IP Office sélectionne une langue lors de sa connexion.
Etiquette d'icône de la barre d'outils	Le système affiche le texte que vous avez indiqué dans ce champ comme étiquette du gadget dans la barre d'outils. Si vous ne précisez pas le texte, le système affiche le nom du gadget entier.
Texte d'infobulle d'icône de la barre d'outils	Le système affiche l'infobulle que vous avez définie dans ce champ pour le gadget donné quand l'utilisateur pointe la souris sur l'icône du gadget dans la barre d'outils.
Icône de la barre d'outils	Le système affiche l'icône que vous avez définie dans ce champ sur la barre d'outils. Assurez-vous que le type d'image soit png, gif ou jpeg seulement, que sa dimension soit de 37*37 pixels et que sa taille maximale soit de 10 Ko. Si vous ne définissez pas d'icône, le système affiche l'image par défaut.
Icône de la barre d'outils sur clic de la souris	Le système affiche l'icône définie dans ce champ quand vous cliquez sur l'icône dans la barre d'outils. Assurez-vous que le type d'image soit png, gif ou jpeg seulement, que sa dimension soit de 37*37 pixels et que sa taille maximale soit de 10 Ko.
Activé	Le système active le gadget pour tous les utilisateurs de one-X Portal for IP Office.
Hauteur du gadget	Le système affiche la hauteur du gadget en fonction de la hauteur que vous avez indiquée dans ce champ. La hauteur par défaut de la fenêtre du gadget est définie à 300 pixels dans ce champ. Vous ne pouvez définir la hauteur de la fenêtre du gadget que lorsque vous ajoutez un gadget. Vous ne pouvez pas modifier la hauteur du gadget après l'avoir ajouté.

3.4.5 Modification d'un gadget externe

Vous pouvez modifier les informations relatives à un gadget, telles que le nom du gadget, l'URL du gadget, le texte affiché dans la barre d'outils, l'infobulle, l'icône affichée dans la barre d'outils et l'icône affichée suite à un clic de la souris.

Pour modifier un gadget externe :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Liste des gadgets externes**.
3. Cliquez sur **Obtenir tout**. Le système affiche une liste de tous les gadgets externes disponibles dans le système.
4. Cliquez sur **Modifier** pour modifier les informations relatives au gadget. Le système affiche la boîte de dialogue **Modifier un gadget**.
5. Reportez-vous au chapitre Ajout d'un gadget externe 64 pour plus d'informations sur les champs du gadget. Effectuez les modifications que vous souhaitez, puis cliquez sur **Enregistrer**.

6. Cliquez sur **Valider les sélections**. Le système met à jour les gadgets externes que vous venez de modifier dans la base de données one-X Portal for IP Office.

3.4.6 Activation d'un gadget externe

Lorsque vous activez un gadget, tous les utilisateurs de one-X Portal for IP Office peuvent ajouter ce gadget.

Pour activer un gadget externe :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Liste des gadgets externes**.
3. Cliquez sur **Obtenir tout**. Le système affiche une liste de tous les gadgets externes disponibles dans le système.
4. Activez le gadget que les utilisateurs de one-X Portal for IP Office pourront ajouter à la fenêtre one-X Portal for IP Office.
5. Cliquez sur **Valider les sélections**. Le système met à jour les gadgets externes que vous venez d'activer dans la base de données one-X Portal for IP Office.

3.4.7 Désactivation d'un gadget externe

Lorsque vous désactivez un gadget, tous les utilisateurs de one-X Portal for IP Office ne peuvent plus ajouter ce gadget à la fenêtre one-X Portal for IP Office. Si vous désactivez un gadget que les utilisateurs ont déjà ajouté à leur fenêtre de one-X Portal for IP Office, le système n'affichera pas le gadget la prochaine fois que les utilisateurs se connecteront.

Pour désactiver un gadget externe :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Liste des gadgets externes**.
3. Cliquez sur **Obtenir tout**. Le système affiche une liste de tous les gadgets externes disponibles dans le système.
4. Désactivez le gadget que vous ne voulez pas que les utilisateurs de one-X Portal for IP Office ajoutent à la one-X Portal for IP Office fenêtre.
5. Cliquez sur **Valider les sélections**. Le système met à jour les gadgets externes que vous venez de désactiver dans la base de données one-X Portal for IP Office.

3.4.8 Suppression d'un gadget externe

Pour supprimer un gadget externe :

1. Cliquez sur **Configuration de gadget** dans le panneau de navigation gauche.
2. Cliquez sur **Liste des gadgets externes**.
3. Cliquez sur **Obtenir tout**. Le système affiche une liste de tous les gadgets externes disponibles dans le système.
4. Sélectionnez le gadget que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.
6. Cliquez sur **Oui** pour confirmer que vous souhaitez effectivement supprimer le gadget. Le système met à jour les gadgets externes que vous venez de supprimer dans la base de données one-X Portal for IP Office.

3.5 Utilisateurs

3.5.1 Ajout/Suppression d'utilisateurs

Le serveur one-X Portal for IP Office est synchronisé avec les utilisateurs figurant sur les systèmes IP Office. L'ajout et la suppression d'utilisateurs se font via la configuration IP Office.

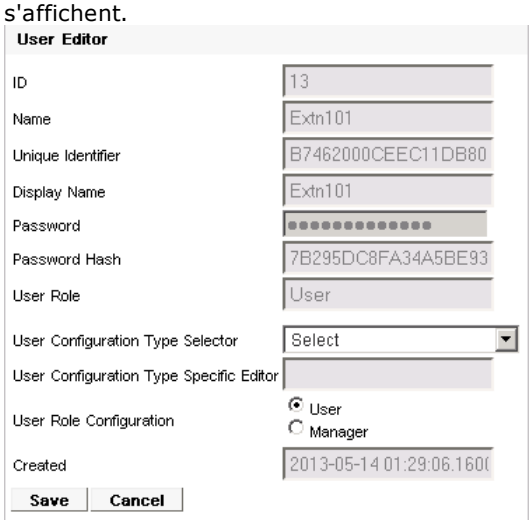
Les modifications apportées aux utilisateurs sur le système IP Office seront appliquées au one-X Portal for IP Office et à d'autres clients Avaya tels que le client de mobilité, Avaya Communicator, etc., 10 minutes après la synchronisation. En outre, les utilisateurs doivent se connecter après la synchronisation.

3.5.2 Modification des paramètres utilisateur

Vous pouvez utiliser les menus d'administration du portail pour afficher et modifier un certain nombre de paramètres utilisateur.

Pour modifier les paramètres utilisateur :

1. Sélectionnez **Configuration**, puis **Utilisateurs**.
2. Cliquez sur **Obtenir tout** et faites défiler les utilisateurs.
3. Cliquez sur le bouton **Modifier** en regard de l'utilisateur à modifier. Les paramètres de configuration utilisateur s'affichent.

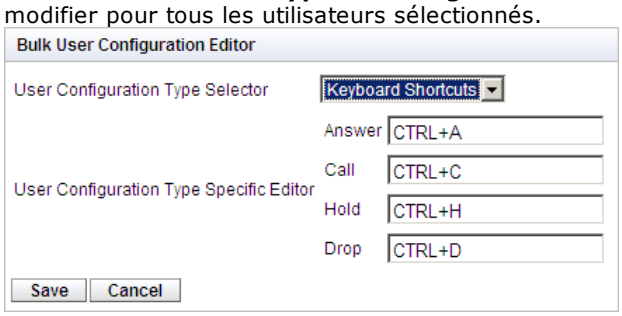


4. Dans le **sélecteur du type de configuration utilisateur**, sélectionnez les paramètres utilisateur à afficher/modifier. Le cas échéant, modifiez les paramètres.
   - **Apparition à l'écran**
     Affiche le lien permettant de télécharger le logiciel d'installation du client de bureau utilisé pour one-X Portal Call Assistant et Outlook Plug-in.
   - **Emplacements**
     Permet de configurer les numéros d'emplacements associés aux boutons de stationnement de l'utilisateur.
   - **Numéro de pont**
     Permet de configurer le numéro de pont pour leurs conférences personnelles.
   - **Mode de télétravail**
     Permet de sélectionner le mode de télétravail de l'utilisateur et la configuration de son numéro de ligne fixe personnelle/de portable à utiliser lorsque le mode est activé.
   - **Configuration de MI/présence**
     Permet de configurer les paramètres de MI/présence de l'utilisateur. Notez que l'utilisateur doit toujours pouvoir activer les notifications via sa propre session one-X Portal for IP Office.
5. Cliquez sur **Enregistrer**.
6. Pour insérer les paramètres modifiés dans la base de données de one-X Portal for IP Office, cochez la case en regard de l'utilisateur, puis cliquez sur **Valider les sélections**.

Pour modifier un lot de paramètres utilisateur :

1. Sélectionnez **Configuration**, puis **Utilisateurs**.
2. Cliquez sur **Obtenir tout** et faites défiler les utilisateurs.
3. Cochez la case en regard de chaque utilisateur à modifier.
4. Cliquez sur **Modifier en bloc**.

5. Dans le **sélecteur du type de configuration utilisateur**, sélectionnez les paramètres de configuration à modifier pour tous les utilisateurs sélectionnés.



6. Une fois les modifications terminées, cliquez sur **Enregistrer**.
7. Sélectionnez la case à côté de chaque utilisateur que vous avez modifié puis cliquez sur **Valider les sélections** pour envoyer les modifications à la base de données one-X Portal for IP Office.

3.6 Annuaires

3.6.1 Ajout d'une source de répertoire LDAP externe

Un fournisseur LDAP est créé par défaut au cours de l'installation, mais il n'est pas configuré pour se connecter à un serveur LDAP (à moins que vous n'optiez pour une installation avancée et modifiiez les paramètres du fournisseur LDAP). La procédure ci-dessous permet de changer les paramètres du fournisseur LDAP pour pouvoir utiliser LDAP.

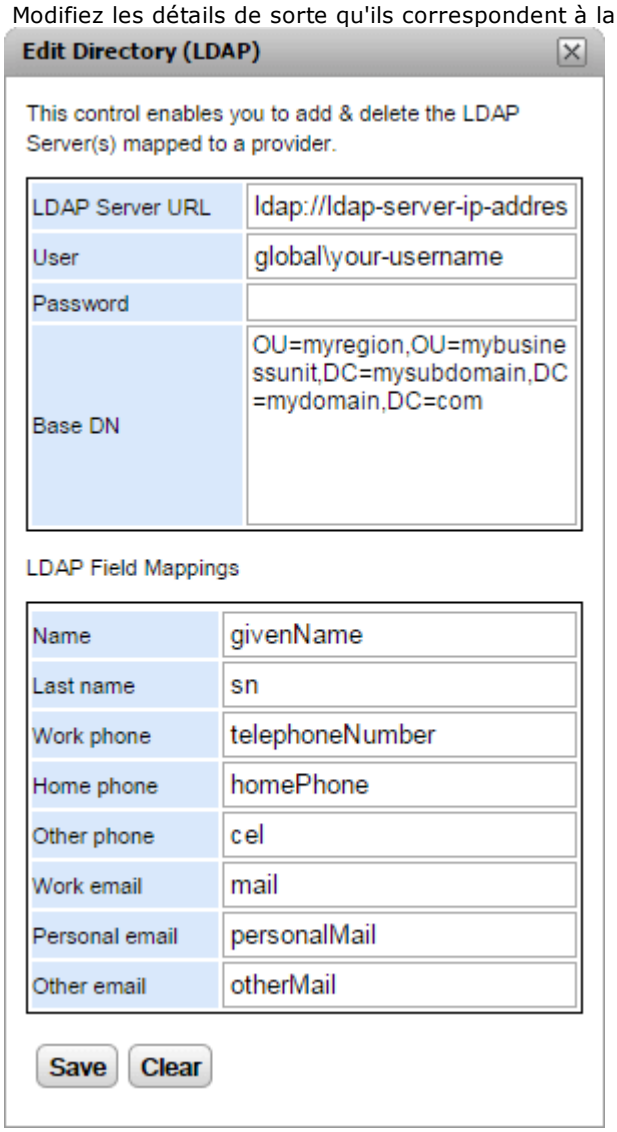
Le fonctionnement de LDAP peut être testé par le biais de l'option **Intégration des répertoires | Recherche dans le répertoire LDAP** 43 dans les menus d'administration.

Contrairement à la prise en charge de LDAP dans le système IP Office, le serveur one-X Portal for IP Office n'importe pas les enregistrements depuis la source LDAP pour ensuite les utiliser en tant que répertoire. Au lieu de cela, lorsqu'un utilisateur de one-X Portal for IP Office saisit des caractères sous l'onglet Répertoire externe du gadget Répertoire, le serveur one-X Portal for IP Office utilise les paramètres de la source LDAP pour rechercher en direct les enregistrements de la source LDAP. Par conséquent, le serveur one-X Portal for IP Office n'a pas besoin de mettre régulièrement à jour ses enregistrements LDAP.

- **Attention**
  Pour ce processus, vous devez redémarrer le service de portail 52 pour que les modifications soient prises en compte. Pendant le redémarrage, il est possible que les utilisateurs ne puissent accéder au portail pendant une durée pouvant atteindre 15 minutes.

Pour ajouter un répertoire LDAP externe :

1. Connectez-vous aux menus d'administration.
2. Sélectionnez **Configuration**, puis **Fournisseurs**.
3. Dans la liste déroulante **Nom du fournisseur**, sélectionnez ***Répertoire (LDAP)***.
4. Cliquez sur l'icône en regard du fournisseur LDAP.
5. Modifiez les détails de sorte qu'ils correspondent à la source du serveur LDAP à utiliser.



- **URL du serveur LDAP**
  URL de la source du répertoire LDAP, par exemple ***ldap:\\ldap.exemple.fr***.
- **Utilisateur/Mot de passe**
  Nom d'utilisateur et mot de passe permettant d'accéder au serveur LDAP.
- **Nom unique de base**
  Également appelé **Base de recherche**. Ce paramètre définit le jeu d'enregistrements de la source LDAP à utiliser pour les recherches. L'administrateur du serveur LDAP fournira une chaîne appropriée, par exemple *ou=Users,dc=global,dc=example,ddc=com*.
- **Mappages des champs LDAP**
  Les noms des champs (à gauche) sont ceux des champs affichés dans le répertoire de one-X Portal for IP Office. Pour chacun d'entre eux, indiquez le nom du champ correspondant dans les enregistrements de la source LDAP.

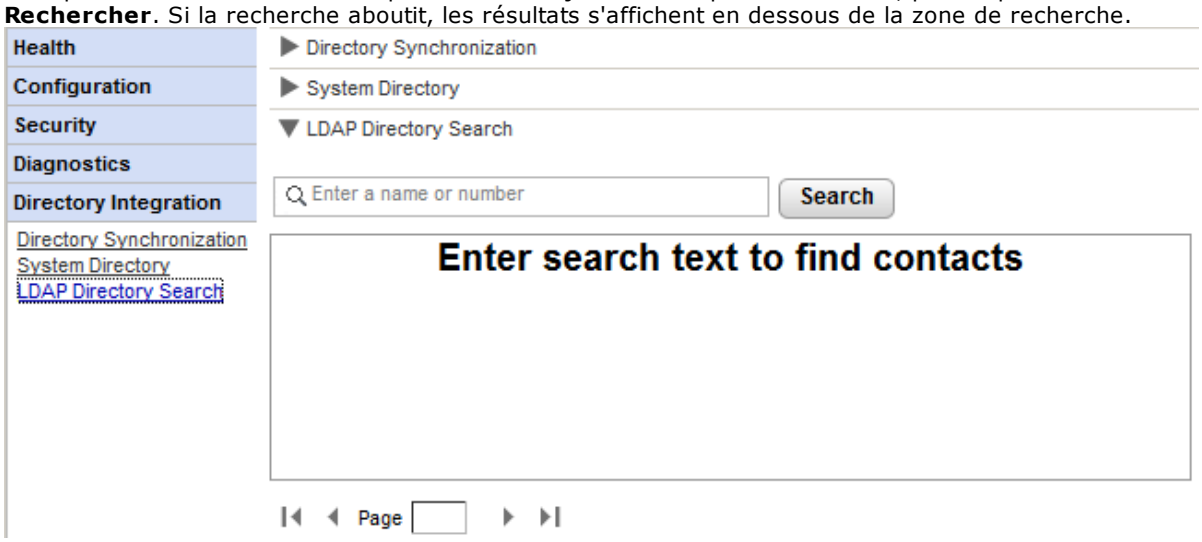
6. Cliquez sur **Enregistrer**.
7. Redémarrez le service one-X Portal Avaya 52.

3.6.2 Vérification du répertoire LDAP externe

Si vous avez configuré une source de répertoire LDAP externe, vous pouvez vérifier que one-X Portal for IP Office peut y accéder à partir des menus d'administration.

Pour vérifier le répertoire LDAP :

1. Sélectionnez **Intégration des répertoires**.
2. Sélectionnez **Recherche dans le répertoire LDAP**.
3. Indiquez un nom ou un numéro qui se trouve déjà dans le répertoire externe, puis cliquez sur **Rechercher**. Si la recherche aboutit, les résultats s'affichent en dessous de la zone de recherche.



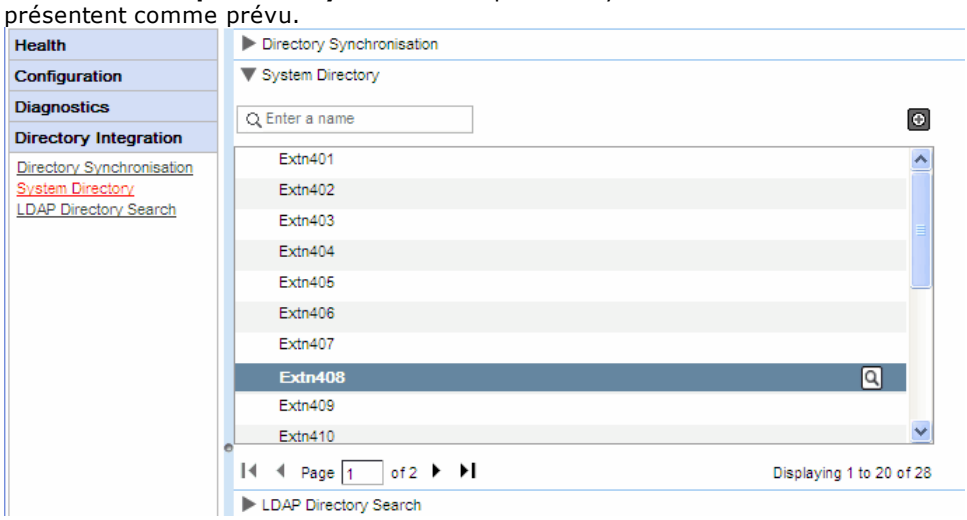
3.6.3 Vérification et mise à jour du répertoire système

Le répertoire système qui s'affiche aux utilisateurs de one-X Portal for IP Office regroupe les utilisateurs, groupes et entrées de répertoire de tous les systèmes IP Office avec lesquels one-X Portal for IP Office est configuré.

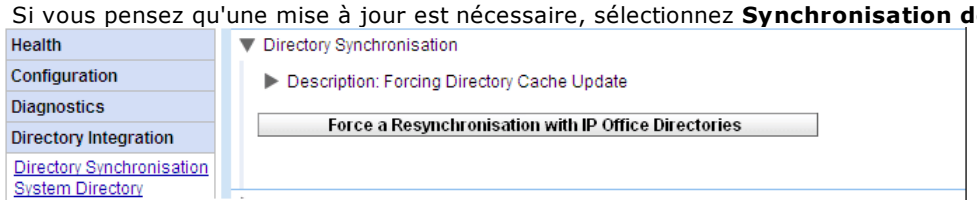
Par défaut, l'application one-X Portal for IP Office met à jour les enregistrements du répertoire système toutes les 300 secondes environ. Les menus d'administration de one-X Portal for IP Office permettent d'afficher le répertoire système et de forcer une mise à jour.

Pour vérifier le répertoire du système :

1. Sélectionnez **Intégration des répertoires**.
2. Sélectionnez **Répertoire système**. Le répertoire système actuel s'affiche. Vérifiez que les entrées se présentent comme prévu.



3. Si vous pensez qu'une mise à jour est nécessaire, sélectionnez **Synchronisation des répertoires**.



4. Cliquez sur **Forcer une nouvelle synchronisation avec les répertoires IP Office**.

3.7 Mise à niveau supérieure/Mise à niveau inférieure

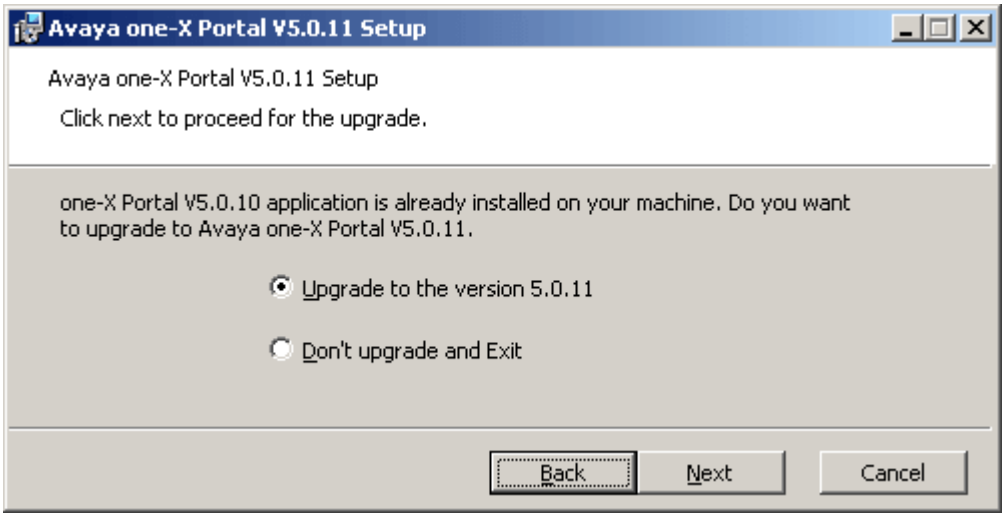
La procédure décrite dans cette section s'applique uniquement aux serveurs Windows.

3.7.1 Mise à niveau de one-X Portal for IP Office

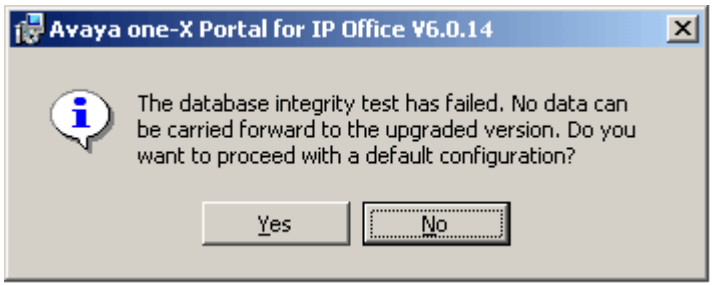
Avant de procéder à la mise à niveau d'un one-X Portal for IP Office sous Windows, veillez à lire le bulletin technique Avaya IP Office sur la version du logiciel one-X Portal for IP Office à installer ou sur la version du logiciel IP Office dans laquelle elle figure. Le bulletin technique inclut des renseignements sur des conditions spéciales et des étapes supplémentaires nécessaires qui ne figurent pas dans la présente documentation.

Si one-X Portal for IP Office est déjà installé sur un PC serveur et que vous exécutez le fichier d'installation d'une version ultérieure, la version existante est détectée et vous êtes invité à indiquer s'il faut la mettre à niveau ou non. Si vous choisissez d'effectuer la mise à niveau, la procédure à suivre ressemble à une installation normale du logiciel. Certaines options d'installation ne sont toutefois pas disponibles lorsqu'il est impossible de modifier les paramètres existants.

- **Attention**
  Pour ce processus, vous devez redémarrer le service de portail 52 pour que les modifications soient prises en compte. Pendant le redémarrage, il est possible que les utilisateurs ne puissent accéder au portail pendant une durée pouvant atteindre 15 minutes.



- S'il est impossible de mettre la base de données existante de one-X Portal for IP Office à niveau, un avertissement s'affiche. Si vous sélectionnez Oui, la base de données existante est remplacée par la base de données par défaut. Si vous sélectionnez Non, vous devez réexécuter le programme d'installation pour rétrograder 73 one-X Portal for IP Office vers la version antérieure compatible avec la base de données.



Au cours du processus de mise à niveau, un fichier de sauvegarde est créé (backup.sql). Il ne s'agit pas d'une sauvegarde complète du système one-X Portal for IP Office. Vous ne devez donc pas l'utiliser pour rétablir des paramètres.

3.7.2 Rétrogradation de one-X Portal for IP Office

Si vous avez mis à niveau le logiciel de l'application one-X Portal for IP Office sous Windows en suivant la procédure de mise à niveau 72, vous pouvez également le mettre au niveau inférieur de la version d'origine installée.

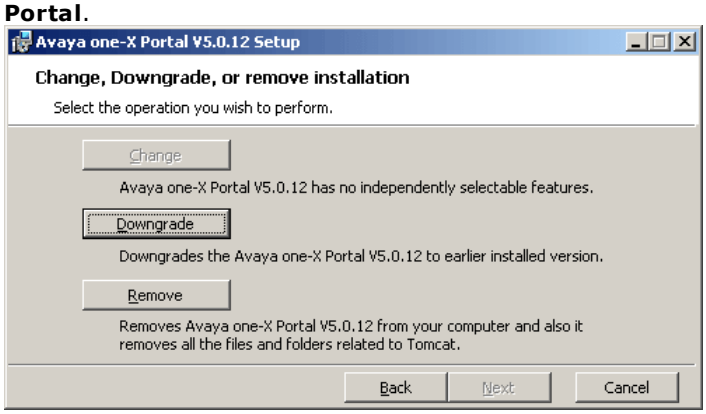
- **Remarque :** L'installation de one-X Portal for IP Office et la dernière mise à niveau de one-X Portal for IP Office apparaissent toutes les deux dans la liste **Ajout/Suppression de programmes** du panneau de configuration de Windows. Notez toutefois que si vous supprimez l'une des deux, l'application entière est désinstallée.

Avant de rétrograder one-X Portal for IP Office, veillez à lire le bulletin technique Avaya IP Office concernant les versions du logiciel one-X Portal for IP Office. Le bulletin technique inclut des renseignements sur des conditions spéciales et des étapes supplémentaires nécessaires qui ne figurent pas dans la présente documentation.

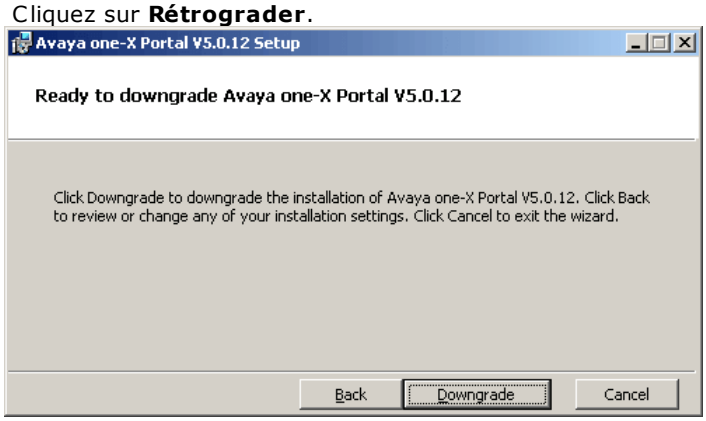
- **Attention**
  Pour ce processus, vous devez redémarrer le service de portail 52 pour que les modifications soient prises en compte. Pendant le redémarrage, il est possible que les utilisateurs ne puissent accéder au portail pendant une durée pouvant atteindre 15 minutes.

Pour la mise à niveau inférieur de one-X Portal for IP Office :

1. Sélectionnez **Démarrer | Tous les programmes | IP Office | one-X Portal | Désinstaller one-X Portal**.



2. Cliquez sur **Rétrograder**.



3. Une fois la rétrogradation terminée, il est nécessaire de redémarrer manuellement 52 le service one-X Portal Avaya.

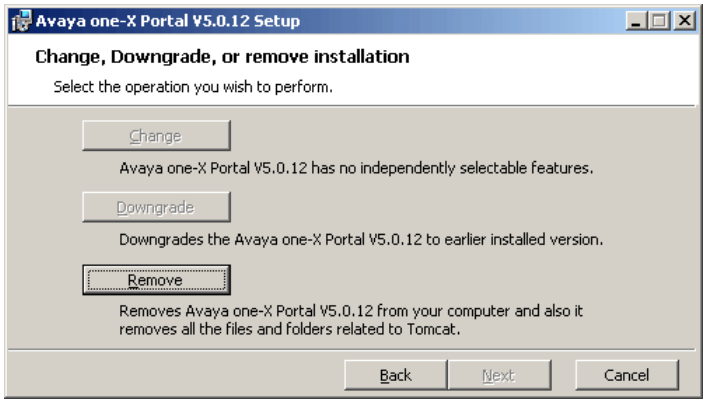
3.7.3 Suppression de one-X Portal for IP Office

Il existe deux méthodes permettant de supprimer l'application one-X Portal for IP Office d'un serveur Windows.

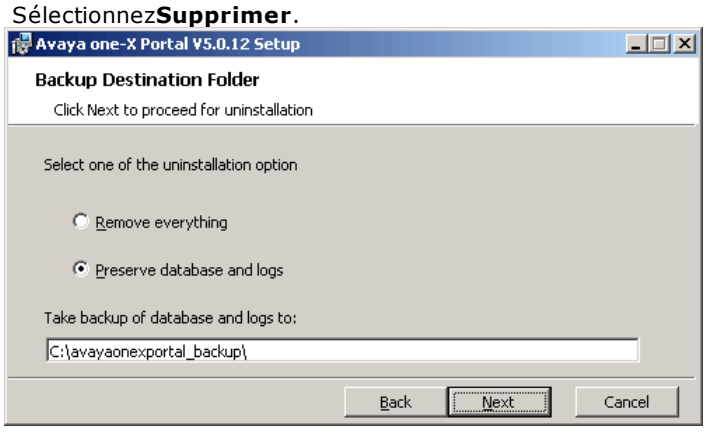
Pour désinstaller one-X Portal for IP Office :

Cette méthode de suppression permet de choisir s'il faut conserver les sauvegardes des fichiers de base de données et journaux.

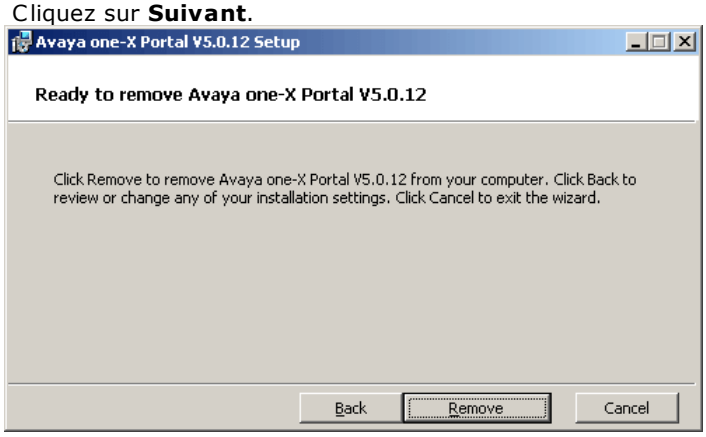
1. Sélectionnez **Démarrer | Tous les programmes | IP Office | one-X Portal | Désinstaller one-X Portal**.



2. Sélectionnez**Supprimer**.



3. Cliquez sur **Suivant**.



4. Cliquez sur **Supprimer** pour commencer à supprimer les fichiers.

Pour supprimer one-X Portal for IP Office via le Panneau de configuration de Windows :

L'option **Ajout/Suppression de programmes** du Panneau de configuration Windows permet de supprimer one-X Portal for IP Office. Cette méthode effectue automatiquement une copie de sauvegarde des fichiers de base de données et journaux dans le dossier ***c:\avayaonexportal_backup***.

1. Ouvrez le Panneau de configuration standard de Windows.
2. Sélectionnez **Ajout/Suppression de programmes**.
3. Sélectionnez **one-X Portal**, puis cliquez sur **Supprimer**.

- Si le logiciel one-X Portal for IP Office a été mis à niveau à un moment ou à un autre, il existe une entrée de programme pour la version one-X Portal for IP Office d'origine et la dernière mise à niveau. Sélectionnez la mise à niveau, puis cliquez sur Supprimer. Cette opération permet de supprimer à la fois la mise à niveau et la version d'origine.

3.8 Messagerie instantanée/Présence

Le serveur one-X Portal for IP Office contient un serveur XMPP en tant que composant, qui est activé par défaut. Ce serveur permet aux utilisateurs de s'envoyer des messages instantanés (MI) et de partager leur présence MI.

L'archivage des messages instantanés est également activé par défaut, ce qui vous permet de rechercher les messages précédemment envoyés par les utilisateurs.

- Configuration du serveur MI 77
- Démarrage du serveur MI 79
- Recherche de l'archive MI 80
- Définition de la durée de l'archivage MI 77
- Intégration du calendrier Exchange 81

Pour désactiver les archives MI :

1. Activation de la console d'administration du serveur XMPP 82
2. Utilisation du serveur XMPP pour désactiver les paramètres d'archivage MI 83
3. Désactivation de la console d'administration du serveur XMPP 83

Pour activer l'archivage MI :

1. Activation de la console d'administration du serveur XMPP 82
2. Utilisation du serveur XMPP pour activer les paramètres d'archivage MI 82
3. Désactivation de la console d'administration du serveur XMPP 83

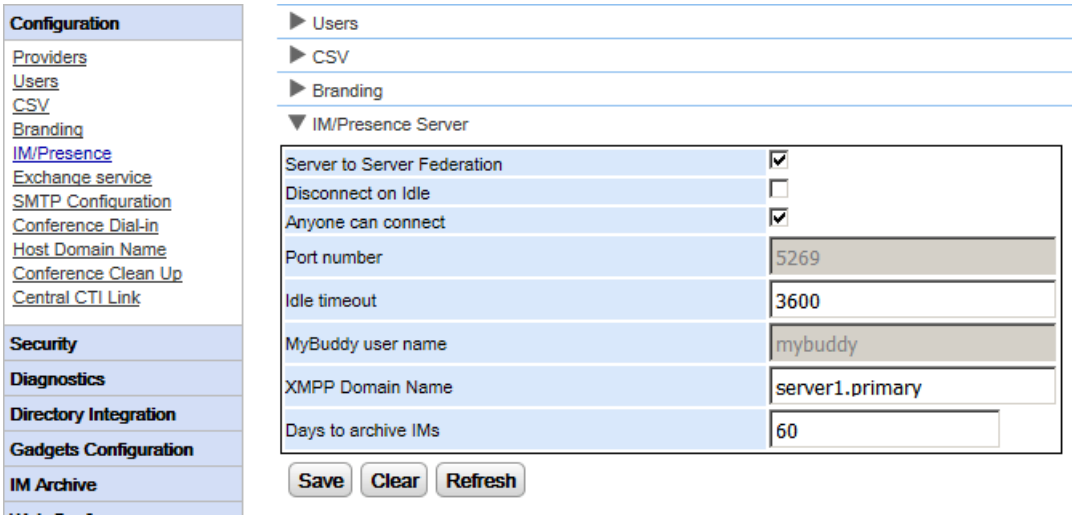
Modifications apportées au fonctionnement XMPP par défaut

Avant IP Office version 9.1, il existait un groupe XMPP par défaut pour chaque système IP Office, dont chaque utilisateur IP Office était membre. Par conséquent, chaque utilisateur pouvait automatiquement voir la présence MI des autres utilisateurs.

Cela n'est plus le cas dans IP Office version 9.1. Pour que les utilisateurs puissent partager leur présence/MI, vous devez créer manuellement des groupes XMPP qui contiennent ces utilisateurs dans la configuration du système IP Office (reportez-vous à l'aide ou à la documentation relative à IP Office Manager).

3.8.1 Configuration du serveur MI

Le portail comprend un composant qui agit comme son serveur de messagerie instantanée/de présence. Le serveur de messagerie instantanée/présence peut être configuré séparément. Voir Serveur de messagerie instantanée/présence 76.



Pour configurer le serveur de messagerie instantanée/présence :

1. Cliquez sur **Configuration** et sélectionnez **Serveur de messagerie instantanée/présence**.
2. Sélectionnez les paramètres serveur requis.
   - **Fédération serveur à serveur**
     Si cette option est sélectionnée, le serveur de présence du portail peut échanger des informations de présence avec d'autres serveurs de présence.
   - **Déconnexion après inactivité**
     Si cette option est activée, les connexions serveur à serveur sont déconnectées si elles restent inactives pendant la période définie dans **Temporisation d'inactivité**.
   - **Tout le monde peut se connecter**
     Permet à tout le monde de se connecter aux services de MI/présence.
   - **Numéro de port**
     Défini sur ***5269***.
   - **Temporisation d'inactivité**
     Durée en seconde définie pour l'option **Déconnexion après inactivité**, si sélectionnée.
   - **Nom d'utilisateur MyBuddy**
     Champ défini sur ***mybuddy***. Cette valeur peut être requise lorsque vous intégrez des informations de présence à d'autres services de MI/présence.
   - **Nom de domaine XMPP**
     Cette option définit le nom de domaine DNS utilisé pour les fonctions de MI/présence :
     - Le nom de domaine XMPP doit être un nom de domaine que le DNS peut résoudre. Vous pouvez définir le nom de domaine XMPP à tout moment. Le nom de domaine doit être accessible depuis Internet si vous souhaitez utiliser la présence en dehors du réseau LAN, par exemple avec one-X Mobile.
     - Avaya recommande l'utilisation d'un serveur DNS partagé de façon à résoudre le nom de votre serveur LAN dans une adresse IP publique du NAT ou du pare-feu, alors qu'il est résolu dans l'adresse IP privée du serveur sur le LAN à l'intérieur de votre réseau.
     - Si vous ne parvenez pas à définir un nom de domaine DNS pouvant être résolu, vous pouvez utiliser l'adresse IP du serveur one-X Portal for IP Office à des fins de MI/présence internes uniquement. Dans ce cas, one-X Portal for IP Office ne peut pas s'associer à des serveurs distants.
     - Pour les serveurs basés sur Linux (IP Office Server Edition, IP Office Application Server et Unified Communications Module), vous devez utiliser les menus Web Control de ces derniers pour configurer leurs paramètres réseau de façon à ce que le lien contenu dans l'e-mail de configuration automatique utilise le nom de domaine FQDN au lieu de l'adresse IP du serveur. Dans Web Control, accédez à Paramètres > Système > Nom de l'hôte pour modifier les paramètres réseau. Si vous modifiez le nom de domaine de toute autre manière, les liens e-mail risquent de ne pas fonctionner correctement.

- **Nombre de jours d'archivage MI**
  Ce champ permet de définir la durée de conservation des messages dans l'archive MI avant leur suppression. La valeur par défaut est 182 jours (6 mois). Si nécessaire, vous pouvez désactiver l'archivage MI83 à l'aide de la console d'administration XMPP. Le serveur de présence/MI doit être disponible (voir État du serveur de présence/MI15) pour modifier ce paramètre.

3. Cliquez sur **Enregistrer**.

3.8.2 Configuration MI utilisateur

Deux utilisateurs de systèmes IP Office ne peuvent voir leur état de présence mutuel et échanger des messages instantanés que s'ils sont membres du même groupe XMPP dans la configuration du système IP Office. Chaque utilisateur peut appartenir à un ou plusieurs groupes XMPP.

Si un nouvel utilisateur IP Office est ajouté par une action simple (ajouter un utilisateur, ajouter un nouvel utilisateur au groupe XMPP, enregistrer la configuration), l'utilisateur n'apparaît pas dans l'affichage portail du groupe XMPP. La solution peut consister à apporter des modifications supplémentaires à la configuration du groupe XMPP ou à redémarrer le service de portail.

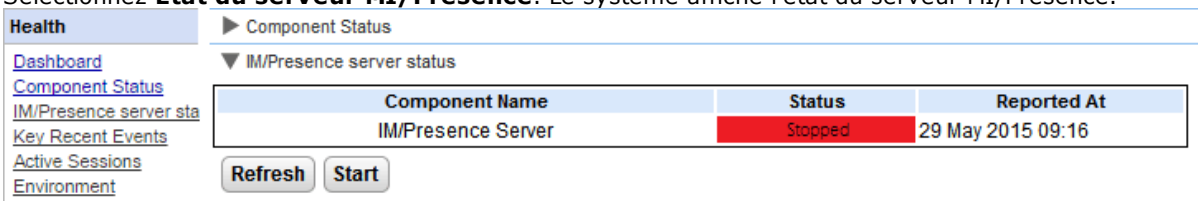
Pour éviter ce problème, il vous est conseillé d'enregistrer la configuration entre chaque action (ajouter un utilisateur, enregistrer la configuration, ajouter un nouvel utilisateur au groupe XMPP, enregistrer la configuration).

3.8.3 Démarrage du serveur MI

Vous pouvez vérifier l'état du serveur MI/Présence via le menu indiquant l'état du serveur MI/Présence 15. Si le serveur MI/Présence n'est pas activé, vous pouvez utiliser la procédure suivante pour démarrer le service.

Pour démarrer le serveur MI/Présence :

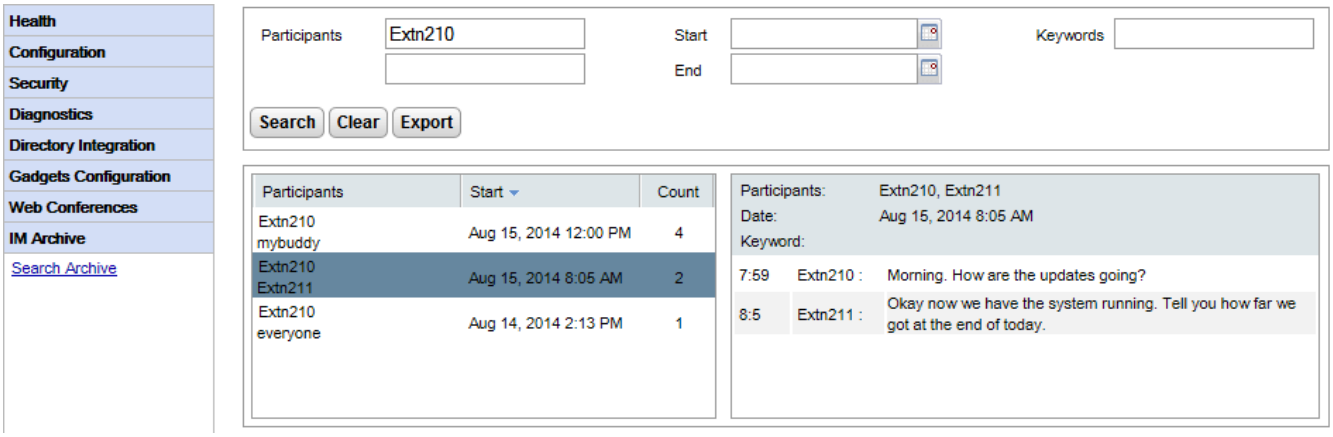
1. Sélectionnez **État d'intégrité**.
2. Sélectionnez **État du serveur MI/Présence**. Le système affiche l'état du serveur MI/Présence.



3. Cliquez sur **Démarrer**.
   - Si la base de données est corrompue, le système affiche le message suivant : *« La base de données du serveur IM/Présence est corrompue et doit être restaurée. Souhaitez-vous la restaurer ? ».*
     - Pour restaurer la base de données et démarrer le serveur MI/Présence, cliquez sur **Oui**. Le système restaure la base de données à partir du dossier de sauvegarde. Le système sauvegarde automatiquement la base de données toutes les huit heures. Vous devez restaurer la base données pour pouvoir démarrer le serveur MI/Présence.
     - Si vous cliquez sur **Non**, le système affiche le message d'avertissement suivant : *« Impossible de démarrer le serveur MI/Présence avec une base de donnée corrompue. Vous ne pourrez pas accéder aux fonctionnalités de MI/Présence ».*

3.8.4 Recherche dans les archives MI

Vous pouvez rechercher des conversations sur les messageries instantanées ayant eu lieu entre les utilisateurs et depuis le système vers un utilisateur.. Tous les champs du volet de recherche sont facultatifs. Le nombre de jours pendant lequel le serveur conserve une conversation MI dans les archives est défini grâce au paramètre **Nombre de jours d'archivage MI** 77.



Pour effectuer une recherche dans les archives MI :

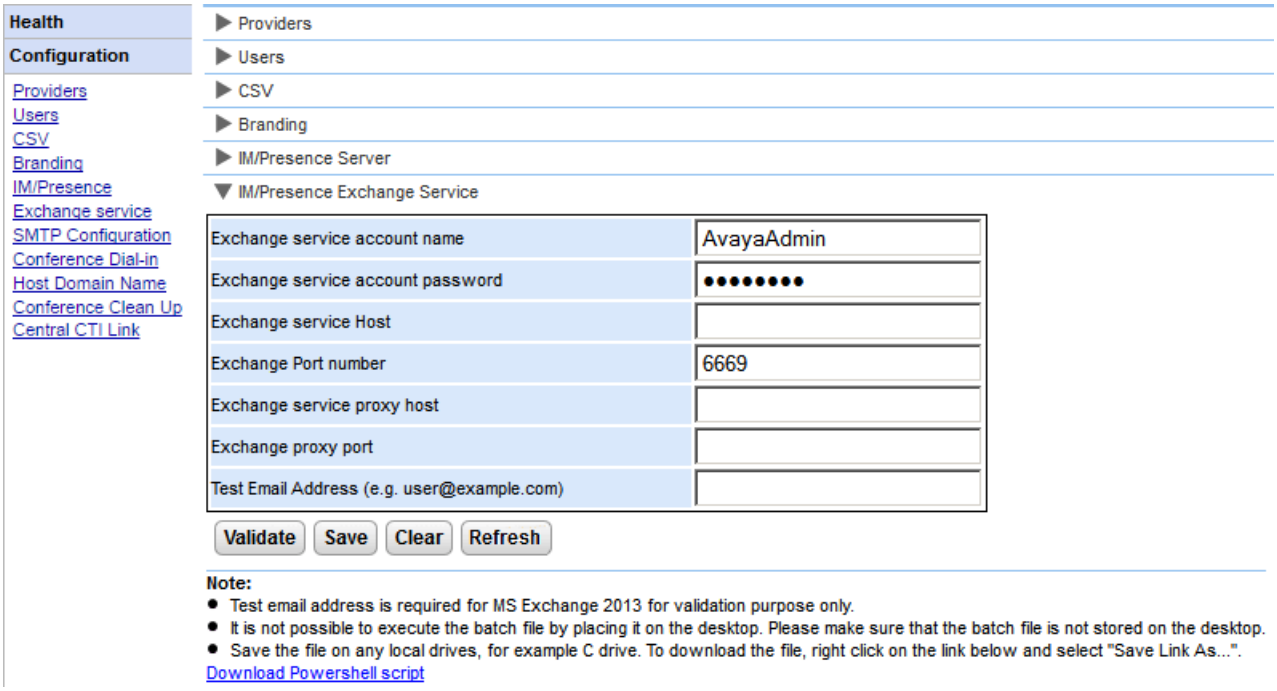
1. Dans le volet de gauche, cliquez sur **Archives MI**.
2. Cliquez sur **Rechercher dans les archives**.
3. Saisissez les critères de recherche, puis cliquez sur Rechercher.

Champ	Description
Participants	Saisissez le nom du participant à la conversation par MI.
Mots clés	Tapez les mots clés dans la conversation MI.
Démarrer	Sélectionnez la date à partir de laquelle vous voulez rechercher les conversations. Si vous ne sélectionnez pas de date, le système affiche les conversations à partir de la plus ancienne conservée par le système.
Fin	Sélectionnez la date des dernières conversations que vous voulez consulter. Si vous ne sélectionnez pas de date, le système affiche les résultats jusqu'à la toute dernière conversation.

4. Cliquez sur la conversation que vous voulez ouvrir. Le système ouvre la conversation.

3.8.5 Intégration du calendrier Exchange

one-X Portal for IP Office peut être configuré avec le serveur Exchange pour exploiter l'exploration de calendrier et les informations de présence des utilisateurs.



Pour configurer les services Exchange :

1. Cliquez sur **Configuration** dans le volet de navigation gauche.
2. Cliquez sur **Service Exchange**.
   a. Entrez ***AvayaAdmin*** comme **nom de compte service Exchange**. Assurez-vous que ce nom soit le même que pour le compte ***AvayaAdmin*** que vous avez créé sur le serveur d'échange.
   b. Entrez le mot de passe qui a été défini pour **AvayaAdmin** comme **mot de passe de compte service Exchange**.
   c. Entrez l'adresse IP de l'hôte du service Exchange dans **Hôte de service Exchange**.
   d. Entrez le numéro de port du service Exchange dans **Numéro du port Exchange**.
   e. Entrez le nom de domaine du serveur proxy utilisé pour connecter le serveur Exchange dans **Hôte proxy du service Exchange**.
   f. Entrez le numéro de port du serveur proxy pour le service Exchange dans **Port proxy Exchange**.
   g. Définissez une **adresse de messagerie électronique d'essai** valide.
3. Cliquez sur **Valider la configuration du service Exchange** pour savoir si les informations Exchange fournies sont valides.
4. Cliquez sur **Enregistrer**.

3.8.6 Activation de la console d'administration XMPP

Par mesure de sécurité, la console d'administration XMPP est désactivée par défaut. Si vous l'activez pour des raisons de maintenance ou de dépannage, vous devez ensuite la désactiver 83 à nouveau.

Pour activer la console d'administration : (Linux)

1. Connectez-vous en tant qu'administrateur.
2. Saisissez `cd /opt/Avaya/oneXportal/openfire/bin`
3. À l'invite, saisissez : `sh AdminConsoleManager.sh enable`
4. Pour redémarrer le service, saisissez : `service onexportal restart`

Pour activer la console d'administration : (Windows)

1. Accédez à l'invite de commande.
2. Allez dans le répertoire d'installation de one-X Portal for IP Office, par exemple cd `C:\Program Files\Avaya\oneXportal`.
   - **Remarque :** Le chemin d'installation est différent sur les systèmes 32 bits et 64 bits
3. Saisissez `cd \openfire\bin`
4. À l'invite de commande, saisissez : `AdminConsoleManager.bat enable`
5. Redémarrez one-X Portal Avaya.

3.8.7 Activation des archives MI

Pour archiver les paramètres d'archivage MI dans le serveur XMPP :

1. Activez la console d'administration XMPP 82.
2. Ouvrez la console d'administration dans un navigateur en saisissant :*http://<adresse IP du serveur>:9094*
3. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe ***admin***.
4. Sélectionnez l'onglet **Serveur**.
5. Sélectionnez l'onglet **Archivage**.
6. Dans le volet de gauche, cliquez sur **Paramètres d'archivage**.
7. Cochez les cases suivantes :
   - **Archivage des états de conversation**
   - **Archivage des sessions de chat entre deux personnes**
   - **Archivage des sessions de chat entre plusieurs personnes**
8. Cliquez sur le bouton **Mettre à jour les paramètres**. Le système enregistre les paramètres, puis affiche le message suivant : *Les paramètres d'archivage ont été enregistrés.*
9. Désactivez la console d'administration XMPP 83.

3.8.8 Désactivation des archives MI

Pour désactiver les archives MI :

1. Activez la console d'administration XMPP 82.
2. Ouvrez la console d'administration dans un navigateur en saisissant :*http://<adresse IP du serveur>:9094*
3. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe ***admin***.
4. Sélectionnez l'onglet **Serveur**.
5. Sélectionnez l'onglet **Archivage**.
6. Dans le volet de gauche, cliquez sur **Paramètres d'archivage**.
7. Décochez les cases suivantes :
   - **Archivage des états de conversation**
   - **Archivage des sessions de chat entre deux personnes**
   - **Archivage des sessions de chat entre plusieurs personnes**
8. Cliquez sur le bouton **Mettre à jour les paramètres**. Le système enregistre les paramètres, puis affiche le message suivant : *Les paramètres d'archivage ont été enregistrés.*
9. Désactivez la console d'administration 83.

3.8.9 Désactivation de la console d'administration XMPP

Par mesure de sécurité, la console d'administration XMPP n'est pas activée par défaut. Si vous l'activez pour des opérations de maintenance ou de dépannage, vous devez ensuite la désactiver à nouveau.

Pour désactiver la console d'administration : (Linux)

1. Connectez-vous en tant qu'administrateur.
2. Saisissez `cd /opt/Avaya/oneXportal/openfire/bin`
3. À l'invite, saisissez : `sh AdminConsoleManager.sh disable`
4. Pour redémarrer le service, saisissez : `service onexportal restart`

Pour désactiver la console d'administration : (Windows)

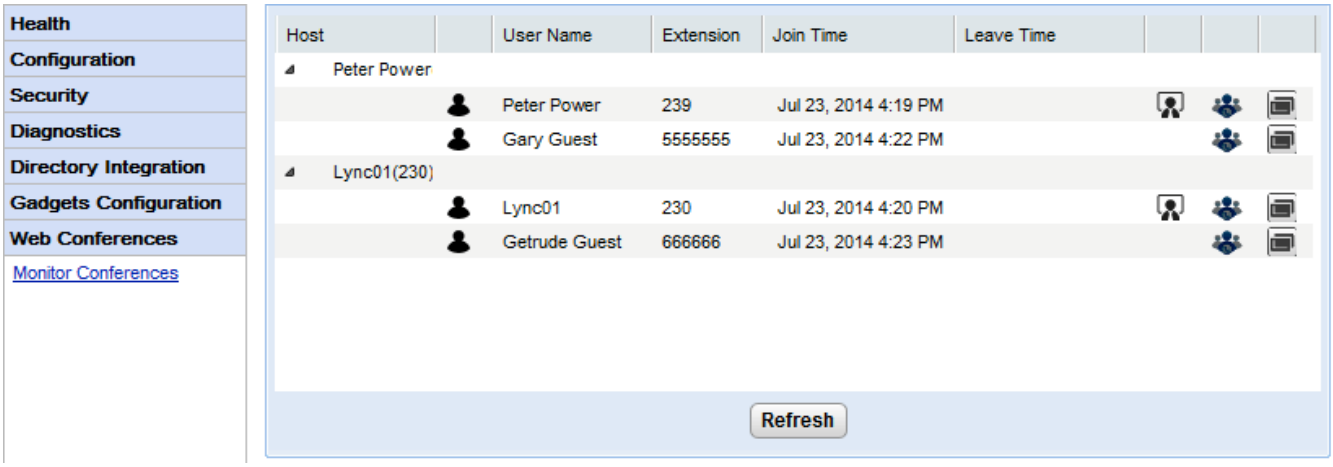
1. Accédez à l'invite de commande.
2. Allez dans le répertoire d'installation de one-X Portal for IP Office, par exemple cd `C:\Program Files\Avaya\oneXportal`.
   - **Remarque :** Le chemin d'installation est différent sur les systèmes 32 bits et 64 bits
3. Saisissez `cd \openfire\bin`
4. À l'invite de commande, saisissez : `AdminConsoleManager.bat disable`
5. Redémarrez one-X Portal Avaya.

3.9 Conférences

Le portail peut comprendre un composant permettant de prendre en charge les fonctions de conférence, de programmation de conférences et les sessions de collaboration Web en même temps que les conférences.

3.9.1 Affichage des conférences

Ce menu permet d'afficher le détail des conférences de collaboration web hébergées par le serveur. Il répertorie les membres participant aux conférences et indique l'heure de leur dernière connexion, ainsi que l'objet de leur participation (présentateurs, membres des conférences audio, membres des conférences web). Ce menu n'est pas pris en charge sur le serveur Unified Communications Module.

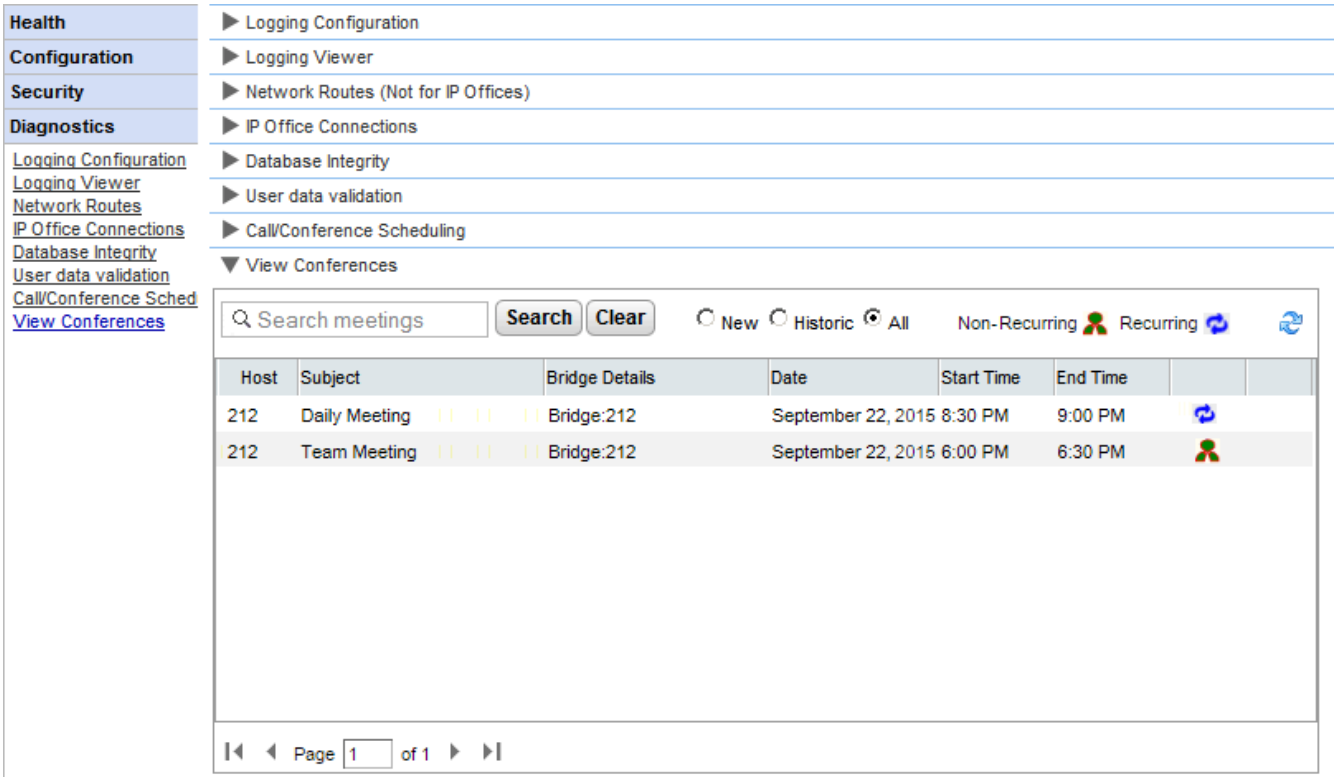


Pour afficher les conférences en cours :

1. Sélectionnez **Conférences Web**, puis **Contrôler les conférences**.
2. Les conférences web en cours figurent dans la liste.
3. Cliquez sur **Hôte** pour agrandir la fenêtre de la conférence et afficher des informations sur les participants.

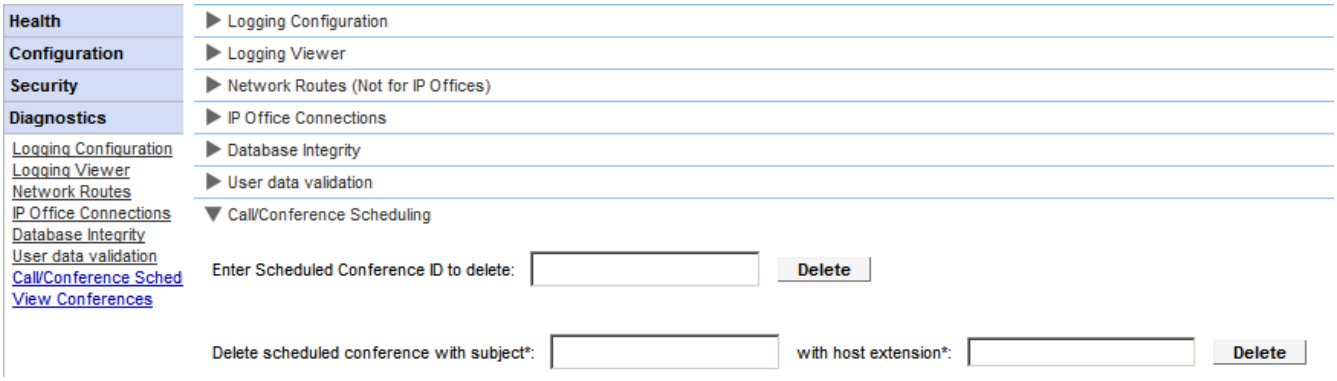
3.9.2 Affichage des conférences planifiées

Ce menu affiche le calendrier des conférences planifiées, sous une forme semblable à celui que les utilisateurs individuels de one-X Portal for IP Office peuvent afficher et utiliser. Il est toutefois différent, dans la mesure où il affiche les conférences planifiées pour tous les utilisateurs. Vous pouvez utiliser ce menu pour supprimer une conférence planifiée ou pour modifier les détails des conférences futures.



3.9.3 Suppression d'une conférence programmée

Vous pouvez supprimer une conférence programmée. S'il s'agit d'une conférence régulière, toutes les occurrences qui lui sont associées seront supprimées également.

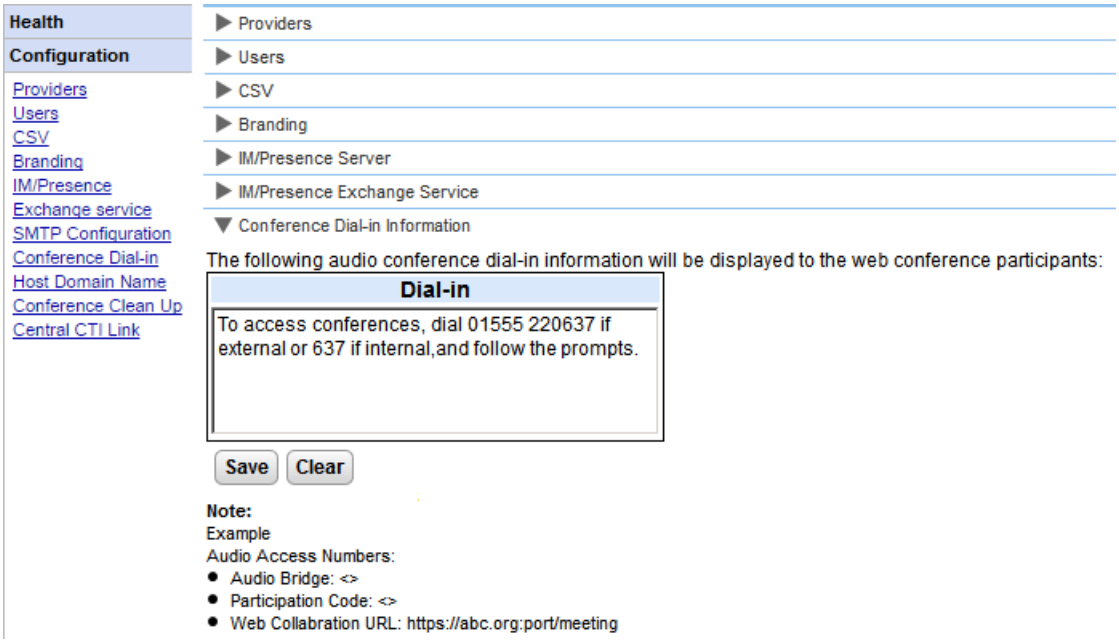


Pour supprimer une conférence ou plusieurs conférences programmées :

1. Cliquez sur **Diagnostics**, puis sélectionnez **Programmation des appels/conférences**.
2. Saisissez l'extension de l'hôte et un objet. Si vous n'indiquez pas d'objet, toutes les conférences programmées par l'hôte seront supprimées.
3. Cliquez sur **Supprimer**.

3.9.4 Message de notification de conférence

Quand un utilisateur programme une conférence, le serveur envoie une notification aux participants conviés par messagerie électronique ou instantanée. Cette notification inclut les détails de la conférence définie par l'utilisateur (numéro de pont, code du participant). Elle peut également comprendre le texte fixe qui a été défini via le menu **Accès entrant conférence**.

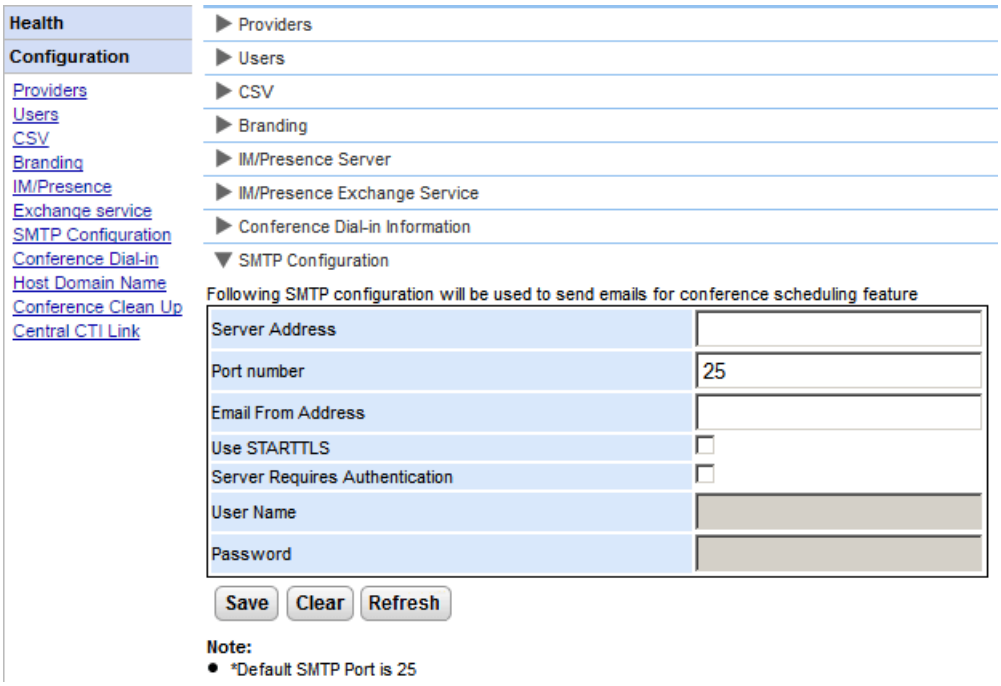


Pour définir le texte de notification :

1. Sélectionnez **Configuration**, puis **Accès entrant conférence**.
2. Saisissez le texte fixe à inclure dans toutes les notifications de conférence.
3. Cliquez sur **Enregistrer**.

3.9.5 E-mails de conférence

Les invitations à des conférences destinées aux utilisateurs peuvent être envoyées par messagerie instantanée ou électronique. Pour un envoi par e-mail, les paramètres associés doivent être configurés ci-dessous. L'adresse e-mail associée à chaque participant est définie dans la configuration du système téléphonique.



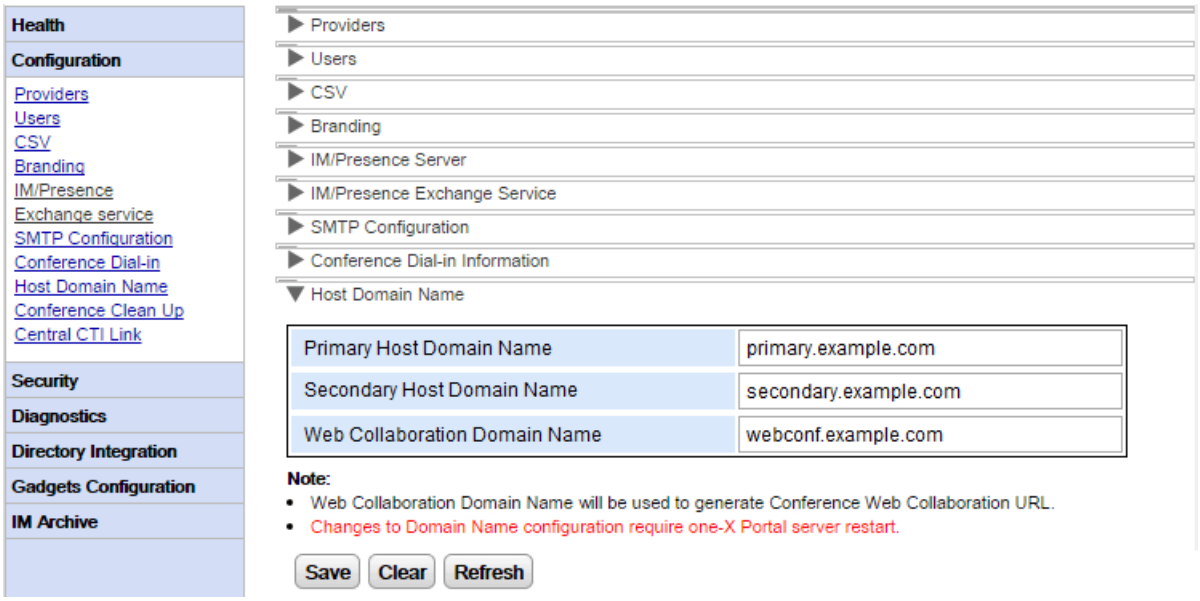
Pour définir le texte de notification :

1. Sélectionnez **Configuration**, puis **Configuration SMTP**.
2. Indiquez les détails e-mail SMTP dont le serveur a besoin :
   - **Adresse du serveur**
     Adresse IP du serveur SMTP du client.
   - **Numéro de port**
     Port d'écoute SMTP du serveur. La valeur par défaut est 25.
   - **Adresse de courrier électronique d'origine**
     Adresse utilisée par le serveur. Certains serveurs ne feront que relayer des messages provenant d'adresses reconnues ou d'adresses du même domaine.
   - **Utiliser STARTTLS**
     Sélectionnez ce champ pour activer l'encodage TLS/SSL. L'encodage permet l'intégration message vocal-email avec des fournisseurs d'emails hébergés qui autorisent uniquement SMTP sur un acheminement sécurisé.
   - **Le serveur doit être authentifié**
     Si le serveur nécessite un compte utilisateur pour recevoir et envoyer des courriers électroniques, saisissez les informations sur le compte configuré sur ce serveur pour qu'IP Office puisse s'en servir.
     - **Nom d'utilisateur**
       Nom de compte à utiliser si l'option Le serveur doit être identifié est sélectionnée.
     - **Mot de passe**
       Mot de passe à utiliser si l'option Le serveur doit être identifié est sélectionnée.
3. Cliquez sur **Enregistrer**.

3.9.6 Définition de l'URL de collaboration Web

Le menu **Configuration | Nom de domaine hôte** est utilisé pour définir le nom de domaine utilisé pour l'accès aux services de portail et entre les serveurs de portail. Le nombre de noms de domaine requis dépend du type de serveur de portail.

Notez que pour que la modification des noms de domaine soit prise en compte, il faut redémarrer le service de portail.

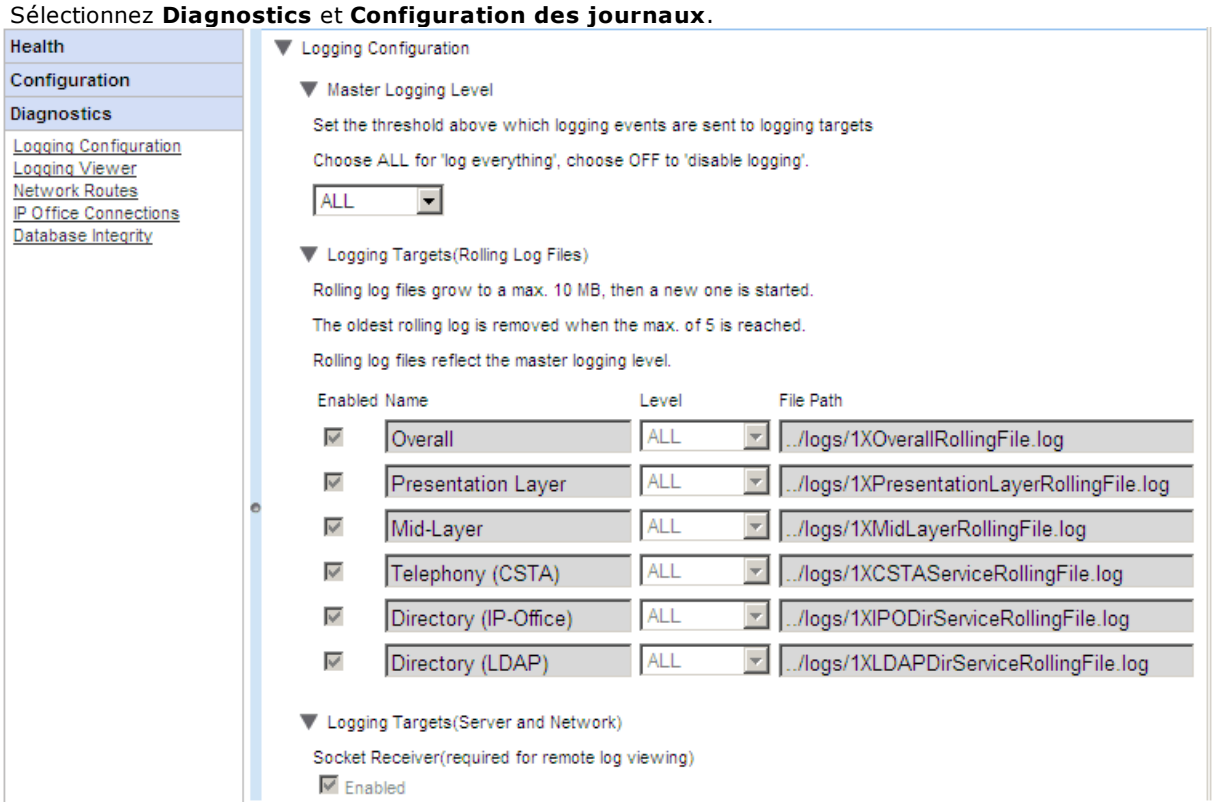


3.10 Consultation des journaux à distance

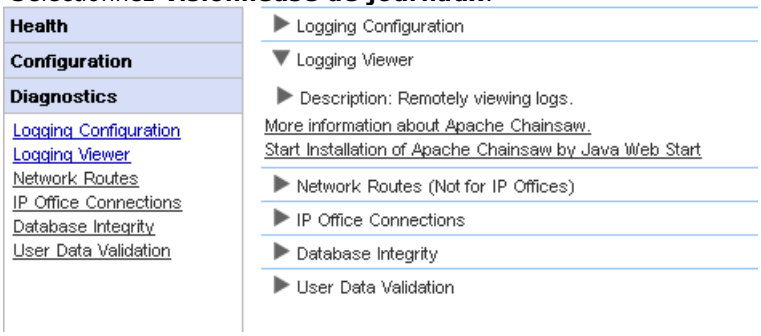
Il est possible de configurer le serveur one-X Portal for IP Office pour que des applications de consignation se connectent sur le port 4560 en vue de recueillir le contenu des fichiers journaux. La sortie se trouve au format Log4j. L'interface de l'administrateur du serveur one-X Portal for IP Office propose des liens permettant d'installer Apache Chainsaw.

Ce processus présume que le PC dispose d'une connexion à Internet. Si ce n'est pas le cas, vous pouvez télécharger et installer Apache Chainsaw en suivant les instructions figurant sur le site Web d'Apache Chainsaw (http://logging.apache.org/chainsaw).

1. Sélectionnez **Diagnostics** et **Configuration des journaux**.

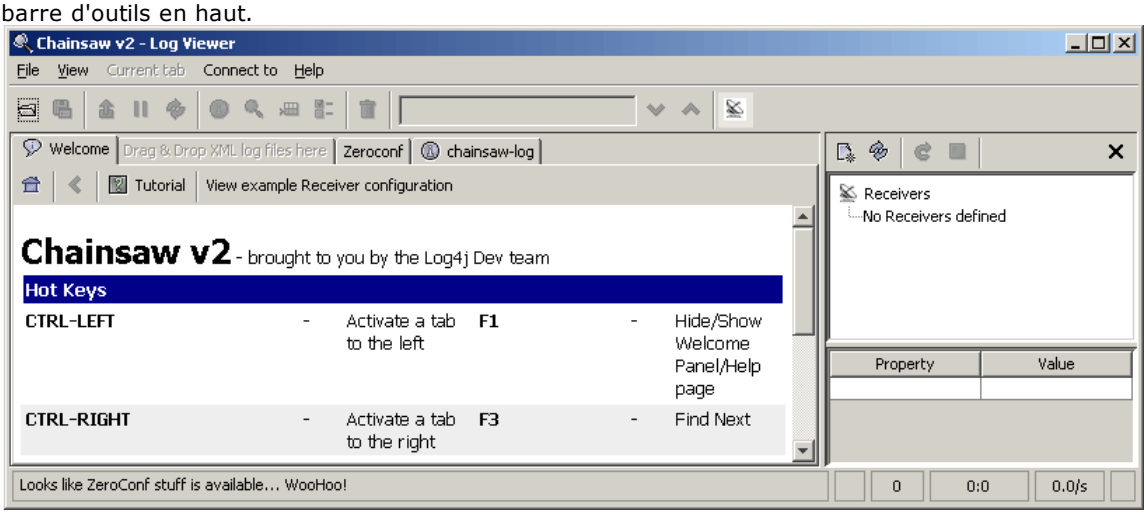


2. Sélectionnez **Consignation des cibles** et vérifiez que l'option **Récepteur de socket** est activée.
3. Sélectionnez **Visionneuse de journaux**.

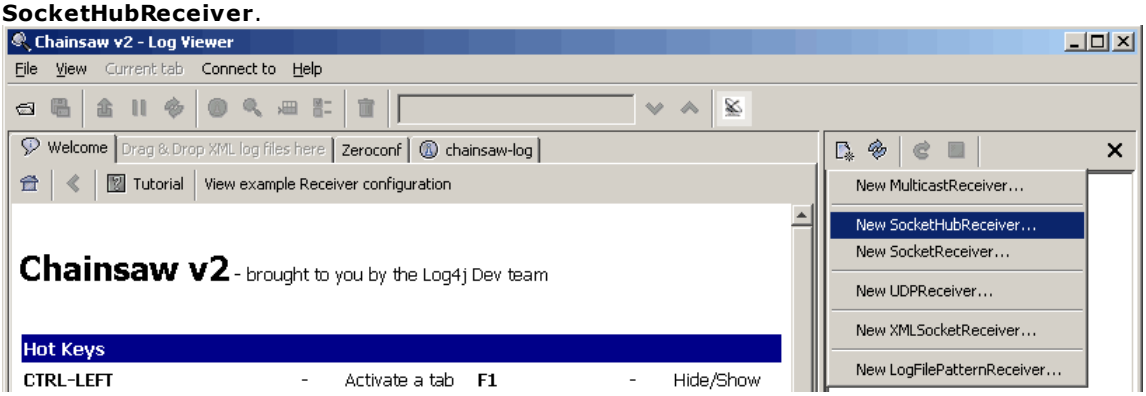


4. Cliquez sur **Lancer l'installation d'Apache Chainsaw via Java Web Start**.
5. La procédure de téléchargement et d'installation de Chainsaw est pratiquement automatique. Chainsaw démarre. Si le message ***Warning: You have no Receivers defined...*** s'affiche, sélectionnez ***I'm fine thanks, don't worry***, ***Don't show me this again***, puis **OK**.

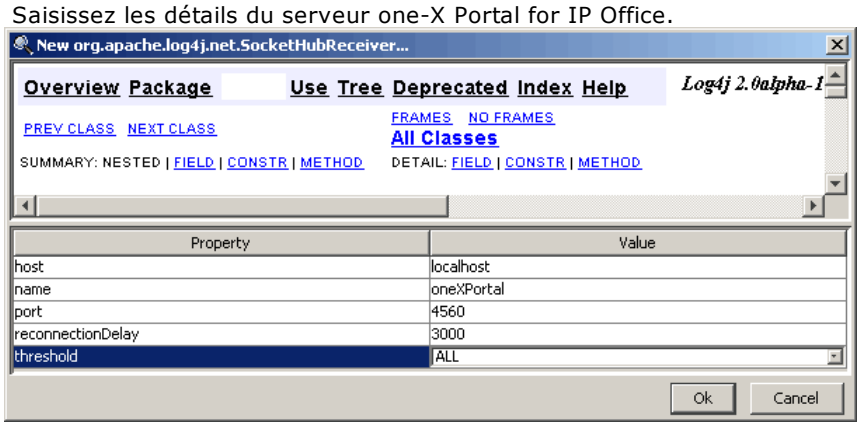
6. Le volet **Récepteurs** s'affiche normalement à droite. Si ce n'est pas le cas, cliquez sur le bouton sur la barre d'outils en haut.



7. Cliquez sur l'icône correspondant à un nouveau récepteur dans le volet Receivers, puis sélectionnez **New SocketHubReceiver**.

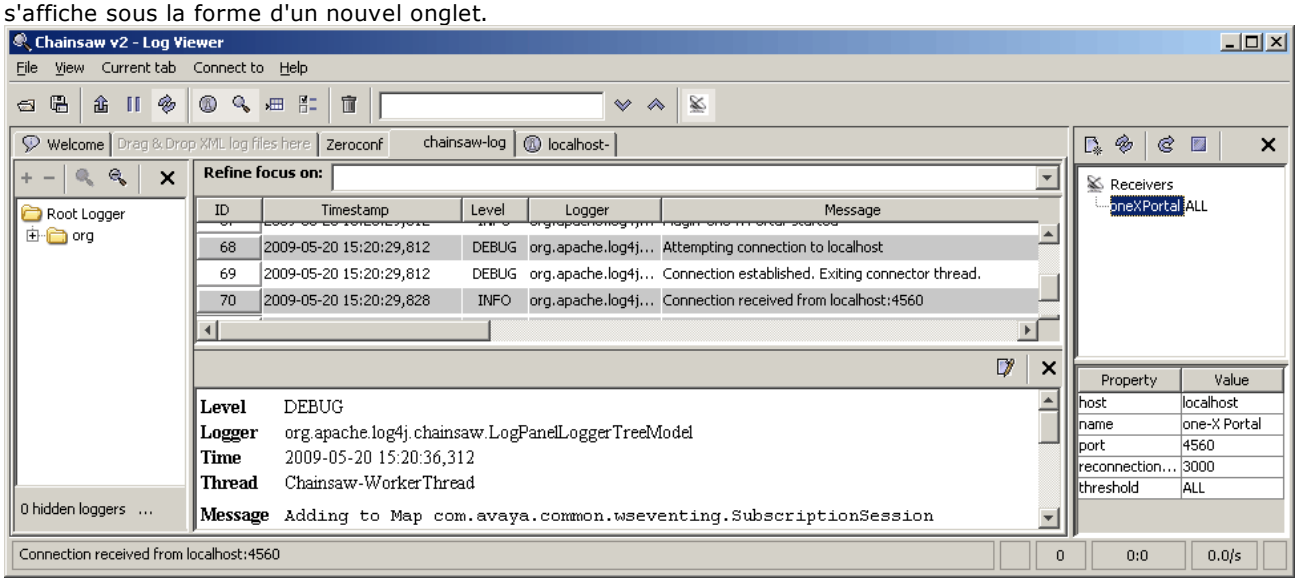


8. Saisissez les détails du serveur one-X Portal for IP Office.

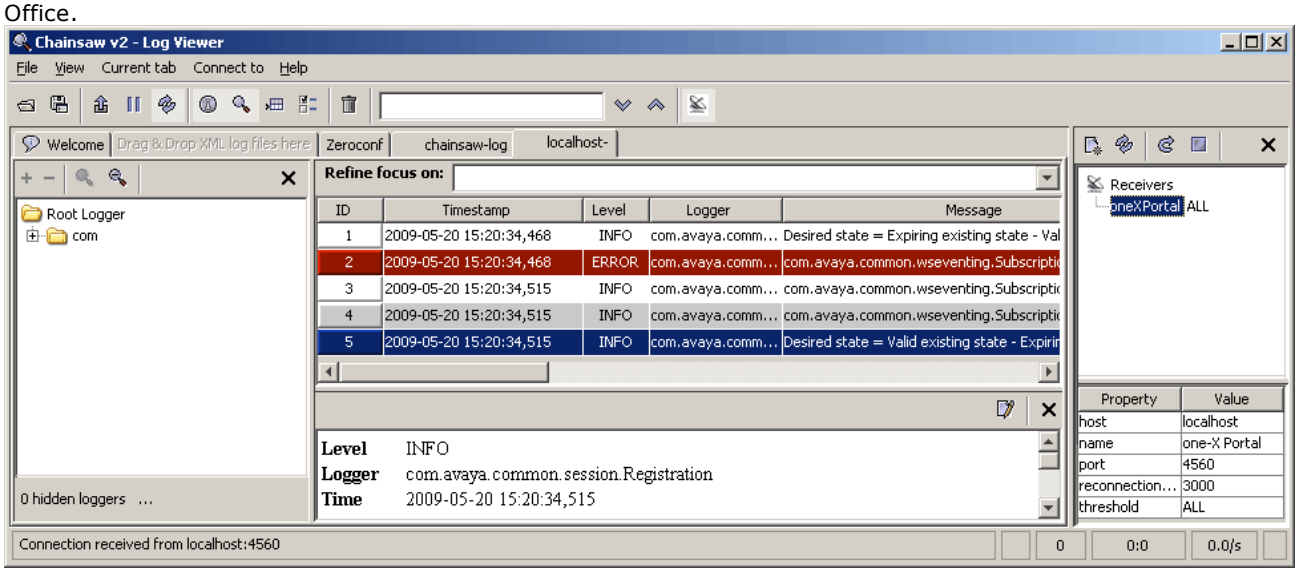


host	Ce champ définit l'adresse du serveur one-X Portal for IP Office. Dans l'exemple ci-dessus, Chainsaw s'exécute sur le PC du serveur one-X Portal for IP Office.
nom	Ce champ n'est utilisé qu'à des fins d'affichage. Saisissez le nom du récepteur dans Chainsaw.
port	Définissez cette valeur sur 4560. Il s'agit du port vers lequel one-X Portal for IP Office envoie les enregistrements des journaux pour qu'ils soient recueillis par les applications de consignation à distance.
reconnectionDelay	Ce champ définit la durée (en millisecondes) pendant laquelle le récepteur doit patienter avant de tenter de se reconnecter s'il pense que sa connexion s'est interrompue.
threshold	Ce champ définit le niveau minimal des messages consignés à recevoir sur All ou Off.

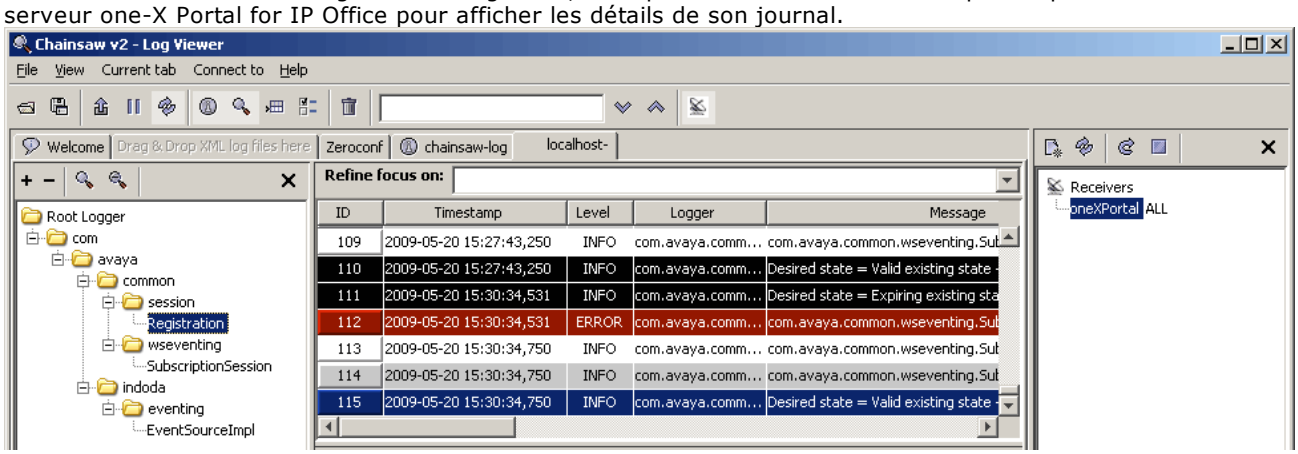
9. Une fois que vous avez renseigné tous les champs, cliquez sur OK. Normalement, après quelques secondes, le récepteur démarre et se connecte au serveur one-X Portal for IP Office. Ce processus apparaît sous la forme d'événements de consignation sous l'onglet de consignation de Chainsaw. Une fois qu'il est terminé, le récepteur s'affiche sous la forme d'un nouvel onglet.



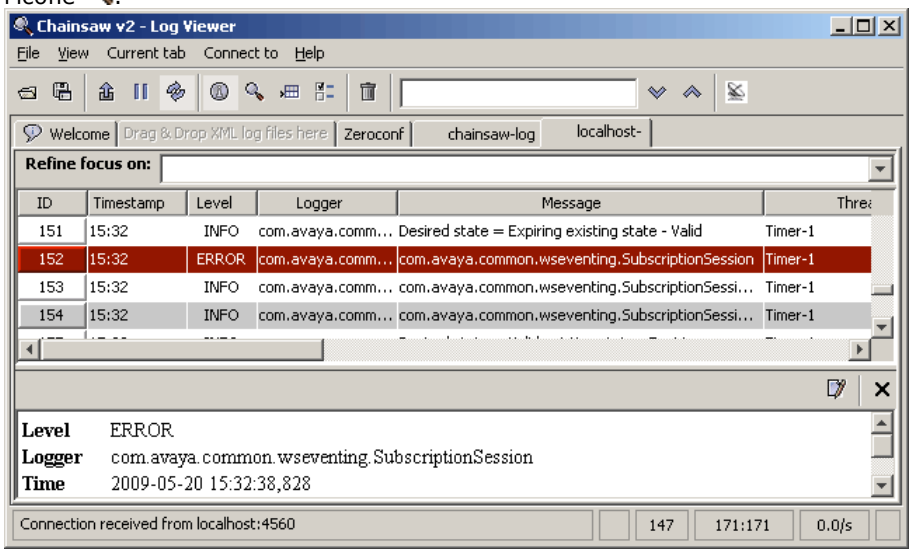
10. Cliquez sur l'onglet du nouveau récepteur pour afficher les enregistrements de consignation one-X Portal for IP Office.



11. Dans l'arborescence de navigation sur la gauche, vous pouvez sélectionner un composant particulier du serveur one-X Portal for IP Office pour afficher les détails de son journal.



12. Pour masquer le volet Receivers, cliquez sur l'icône . Pour masquer l'arborescence de navigation, cliquez sur l'icône .



3.11 Dépannage

Problème de version non concordante

Symptômes	• Le contrôle d'intégrité de la base de données 39 échoue. • Au démarrage de one-X Portal for IP Office, la version indiquée sur la page de connexion correspond à la version précédente et diffère de celle indiquée dans Windows (menu **Démarrer | Programmes | IP Office | Avaya one-X Portal for IP Office | Désinstaller V***X.XX*).
Cause	Généralement, le programme d'installation de one-X Portal for IP Office arrête automatiquement tout serveur Web Tomcat associé à une installation antérieure de one-X Portal for IP Office. Mais cela n'est pas toujours le cas : il arrive qu'il ne parvienne pas à arrêter le serveur Tomcat, mais qu'il indique néanmoins que le processus d'installation s'est terminé avec succès. Dans ce cas, les versions utilisées par les composants sont différentes.
Résolution	1. Supprimez one-X Portal for IP Office 74. 2. Supprimez manuellement le dossier de l'application one-X Portal for IP Office (par défaut, il s'agit de C:\Program Files (x86)\Avaya\onexportal). Vous devez redémarrer le serveur si le dossier est verrouillé. 3. Installez la nouvelle version de one-X Portal for IP Office.

one-X Portal for IP Office Ne démarre pas

Symptômes	• Le démarrage de one-X Portal for IP Office échoue. • Le message **Prorun Error** est consigné dans les fichiers journaux du serveur Tomcat. • L'exécution d'autres applications Java sur le serveur (IP Office System Status Application, par exemple) échoue.
Résolution	1. Vérifiez s'il existe un conflit de ports. Si c'est le cas, éliminez l'autre application ou installez one-X Portal for IP Office sur un autre port. 2. A l'aide de l'applet **Ajout/Suppression de programmes** de Windows, supprimez Java. 3. Supprimez one-X Portal for IP Office 74. 4. Installez one-X Portal for IP Office.

3.12 Ajouter des administrateurs supplémentaires

- Par défaut les serveurs one-X Portal for IP Office sous Linux utilisent l'**authentification référée**. Cela signifie que les droits d'administration du portail sont attribués aux utilisateurs de sécurité configurés dans la configuration de sécurité du service IP Office exécuté sur le même serveur. Il s'agit par défaut de l'utilisateur **Administrateur**, mais il est possible de configurer des utilisateurs de service supplémentaires qui pourront accéder à l'administration du portail.
- Si l'authentification référée est désactivée, le portail utilise son propre compte d'administration local de la même manière que sur un serveur Windows, tel que décrit ci-dessous.

Le processus ci-dessous explique comment configurer les droits d'administration du portail pour des utilisateurs supplémentaires des services de sécurité. Chaque utilisateur du service IP Office est le membre d'un ou de plusieurs groupes de droits. Les paramètres du groupe de droits permettent de définir les options disponibles pour l'utilisateur du service, notamment son niveau d'accès au serveur one-X Portal for IP Office.

Pour afficher et régler les paramètres du groupe de droits :

1. Dans IP Office Manager, sélectionnez **Fichier | Avancé | Paramètres de sécurité**.
2. Sélectionnez le système IP Office et cliquez sur **OK**.
3. Saisissez le nom d'utilisateur et le mot de passe permettant d'accéder aux paramètres de sécurité du système IP Office.
4. Sélectionnez  **Groupes de droits**.
5. Sélectionnez l'onglet **Externe**. Cet onglet comprend les paramètres permettant de définir le niveau d'accès au portail accordé aux membres du groupe de droits.
   - **Administrateur de One-X Portal**
     Ce niveau permet d'accéder aux menus réservés à l'administrateur du portail.
   - **Super utilisateur de One-X Portal**
     Ce niveau permet d'accéder aux menus AFA du portail.
6. Sélectionnez un groupe de droits particulier dans la liste pour voir de quel niveau d'accès dispose le groupe de droits.
7. Si vous apportez des modifications, cliquez sur **OK**.
8. Cliquez sur  pour enregistrer les modifications.

Pour modifier l'adhésion d'un utilisateur du service au groupe de droits :

1. Dans IP Office Manager, sélectionnez **Fichier | Avancé | Paramètres de sécurité**.
2. Sélectionnez le système IP Office et cliquez sur **OK**.
3. Saisissez le nom d'utilisateur et le mot de passe permettant d'accéder aux paramètres de sécurité du système IP Office.
4. Sélectionnez  **Utilisateur du service**.
5. Sélectionnez l'utilisateur du service. Les informations affichent le groupe de droits dont cet utilisateur du service est membre.

Chapitre 4.
Menus AFA

4. Menus AFA

one-X Portal for IP Office prend en charge une série de menus pour la sauvegarde et la restauration des paramètres de configuration de one-X Portal for IP Office. Ils permettent d'effectuer des opérations de sauvegarde et restauration en utilisant le serveur one-X Portal for IP Office, un serveur FTP ou votre propre PC comme destination des fichiers de sauvegarde.

Les menus doivent également autoriser la sauvegarde et la restauration entre une nouvelle et une ancienne installation de one-X Portal for IP Office sur un nouveau serveur. La sauvegarde et la restauration entre différentes versions de one-X Portal for IP Office, par exemple de la version 6.1 à 7.0, ne sont cependant pas prises en charge.

L'accès aux menus de sauvegarde et restauration avancés est contrôlé par un utilisateur différent et un mot de passe provenant d'un autre accès administrateur.

- **Serveurs Linux**
  Lorsque le portail est exécuté sur un serveur Linux, le portail peut être inclus dans les fonctions de sauvegarde et de restauration disponibles dans les menus de gestion Web du serveur Linux. Ces options comprennent la prise en charge de la sauvegarde sur les serveurs HTTP. HTTPS et SFTP et les sauvegardes programmées.

4.1 Se connecter

Un seul utilisateur peut être connecté à la fois en temps que Superutilisateur.

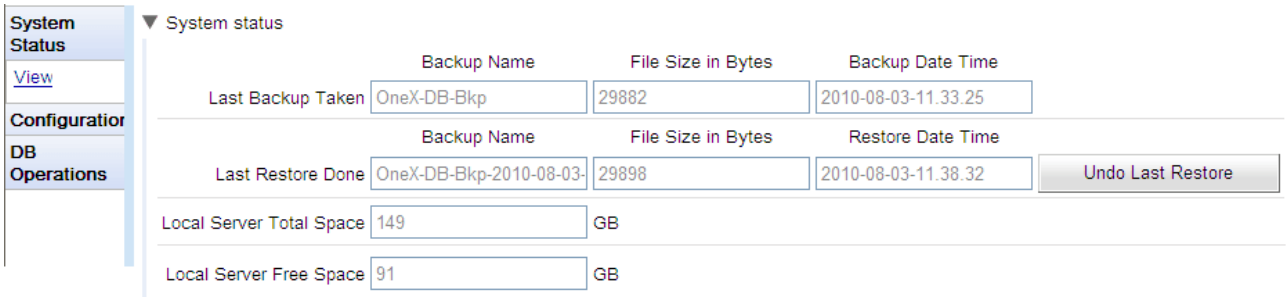
- Par défaut les serveurs one-X Portal for IP Office sous Linux utilisent l'**authentification référée**. Cela signifie que les droits d'administration du portail sont attribués aux utilisateurs de sécurité configurés dans la configuration de sécurité du service IP Office exécuté sur le même serveur. Il s'agit par défaut de l'utilisateur **Administrateur**, mais il est possible de configurer des utilisateurs de service supplémentaires qui pourront accéder à l'administration du portail.
- Si l'authentification référée est désactivée, le portail utilise son propre compte d'administration local de la même manière que sur un serveur Windows, tel que décrit ci-dessous.

Pour vous connecter :

1. Saisissez l'adresse dans la barre d'adresse du navigateur ***http://<nom du serveur>:<port du serveur>/onexportal-afa.html***, où :
   - ***<nom du serveur>*** est le nom ou l'adresse IP du serveur one-X Portal for IP Office.
   - ***<port du serveur>*** est le numéro de port utilisé par one-X Portal for IP Office. Il peut s'agir du port 9443 ou du port 8443 pour l'accès HTTPS.
   - Vous pouvez utiliser ***http://*** plutôt que ***https://*** et ***8080*** comme port si un accès non sécurisé a été configuré. Voir Protocole 34.
   - Vous pouvez également sélectionner **Connexion AFA** à partir du menu de connexion de l'utilisateur normal.
2. Dans le menu de connexion, entrez le mot de passe :
   - Sur un serveur Linux, entrez le mot de passe d'un utilisateur du service de sécurité IP Office configuré avec un accès de Super Utilisateur à one-X Portal 94. Par défaut, il s'agit de l'utilisateur **Administrateur**.
   - Sur un serveur Windows, entrez le nom ***Super Utilisateur*** et le mot de passe associé.
     - Quand vous vous connectez pour la première fois, utilisez le mot de passe par défaut ***MyFirstLogin1_0***. Une fois connecté, un message vous invitera à saisir un nouveau mot de passe pour le compte du ***Super utilisateur*** ainsi que des informations supplémentaires.
   - **Nom d'affichage**
     Saisissez un nom à afficher dans les menus one-X Portal for IP Office.
   - **Mot de passe / Confirmer Mot de passe**
     Saisissez un mot de passe qui sera utilisé pour accéder ultérieurement au ***Superutilisateur***. Ce mot de passe est utilisé sur les serveurs Windows et les serveurs Linux n'utilisant pas l'**authentification référée**.

4.2 État du système

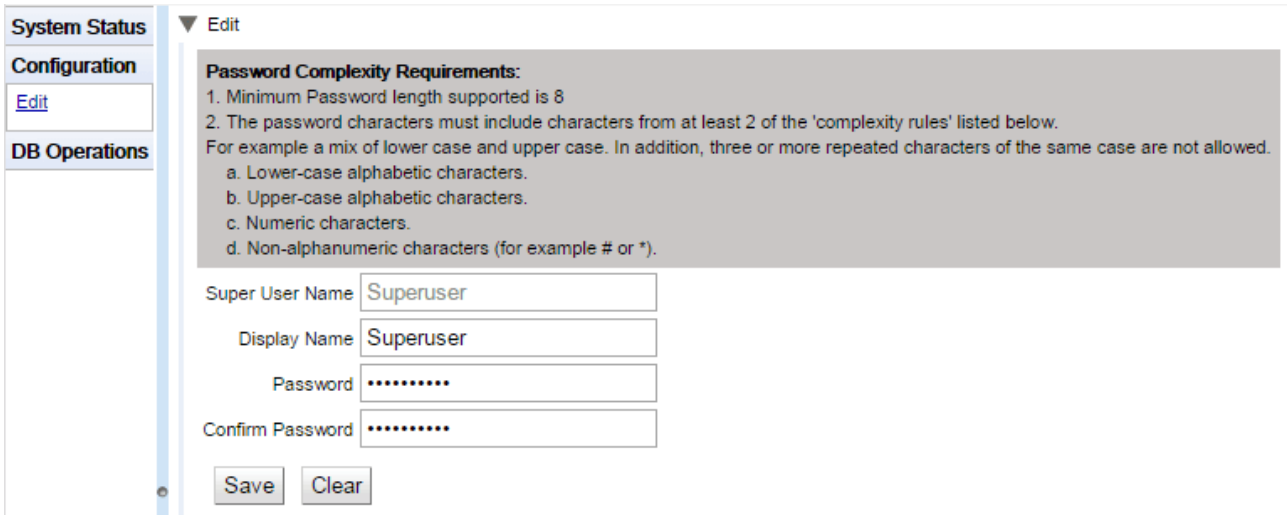
Ce menu récapitule l'usage précédent des menus du Superutilisateur. Il permet également de revenir à la dernière restauration précédente.



- **Dernière sauvegarde prise**
  Cette section décrit la dernière sauvegarde prise en passant par le menu de sauvegarde. Le nom du fichier de sauvegarde est un fichier zip dont le nom est basé sur le **Nom de la sauvegarde** et la **Date et l'heure de la sauvegarde**. Par exemple, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Dernière restauration effectuée**
  Cette section décrit la dernière restauration effectuée. La date et l'heure de la restauration sont indiquées dans le nom du fichier utilisé pour cette opération. La commande Annuler la dernière restauration permet de revenir à l'action de restauration.
- **Espace total du serveur local**
  Indique l'espace approximatif sur le disque du serveur one-X Portal for IP Office.
- **Espace libre du serveur local**
  Indique l'espace libre approximatif restant sur le disque du serveur one-X Portal for IP Office.

4.3 Configuration

Ce menu permet de configurer les paramètres de base pour l'accès du ***superutilisateur***.



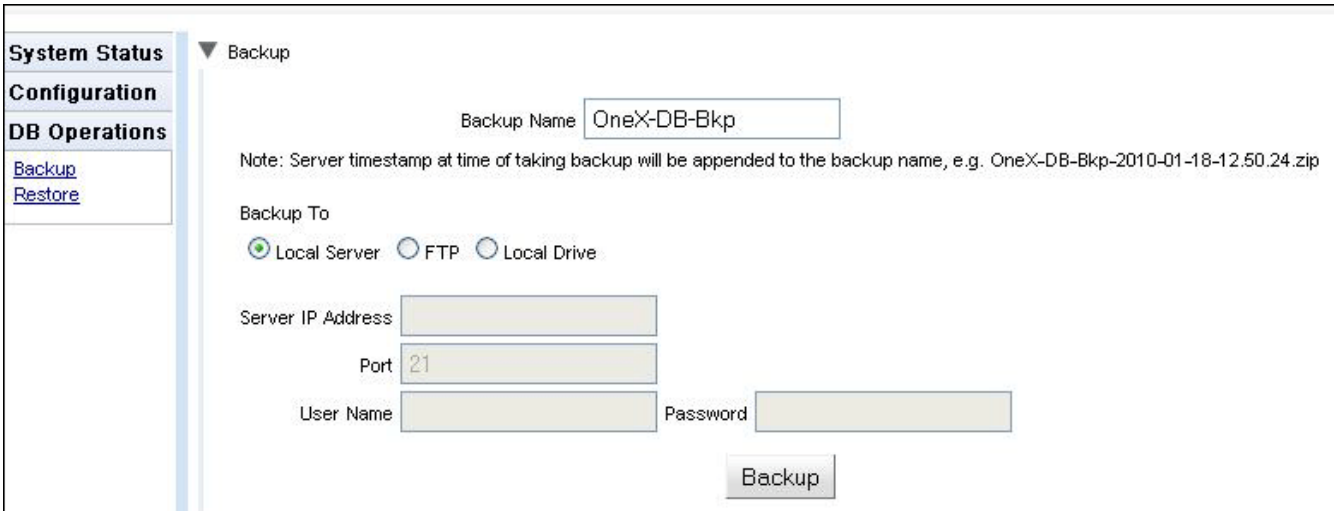
- **Nom du superutilisateur**
  Il s'agit d'un nom fixe qui ne peut pas être modifié.
  - **Nom d'affichage**
    Saisissez un nom à afficher dans les menus one-X Portal for IP Office.
  - **Mot de passe / Confirmer Mot de passe**
    Saisissez un mot de passe qui sera utilisé pour accéder ultérieurement au ***Superutilisateur***. Ce mot de passe est utilisé sur les serveurs Windows et les serveurs Linux n'utilisant pas l'**authentification référée**.

4.4 Fonctionnements DB

Les menus permettent de créer des fichiers de sauvegarde et de restaurer les paramètres d'un fichier de sauvegarde précédent.

4.4.1 Sauvegarde

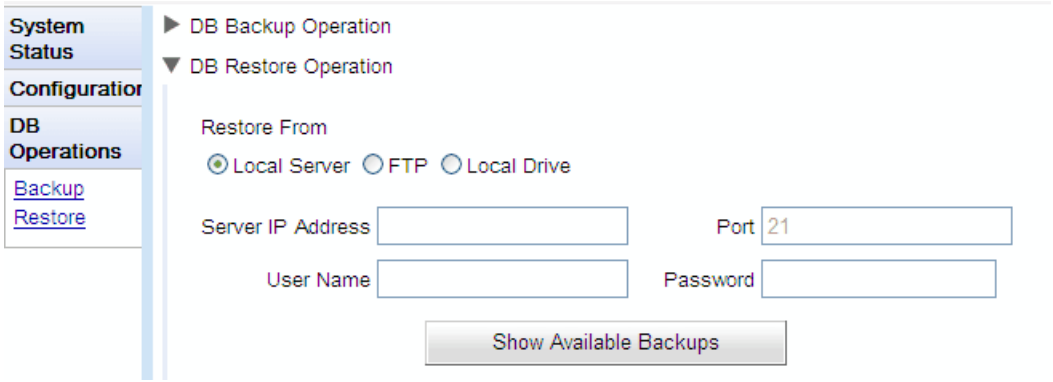
Ce menu permet de créer des fichiers de sauvegarde.



- **Nom de sauvegarde**
  Il s'agit du nom des fichiers zip de sauvegarde. La date et l'heure de la sauvegarde sont également ajoutées au nom du fichier. Par exemple, ***OneX-DB-Bkp-2010-08-03-11.33.25.zip***.
- **Sauvegarde sous**
  Ce paramètre permet de sélectionner la destination du fichier de sauvegarde.
- **Serveur local**
  Si cette option est sélectionnée, le fichier de sauvegarde est créé dans le **Dossier de sauvegarde**.
- **FTP**
  Si cette option est sélectionnée, le fichier de sauvegarde est créé temporairement dans le **Dossier de sauvegarde**. Il est ensuite envoyé à l'adresse du serveur FTP indiquée.
- **Lecteur local**
  Si cette option est sélectionnée, le fichier de sauvegarde est créé temporairement dans le **Dossier de sauvegarde**. Le navigateur propose ensuite de le télécharger.
- **Paramètres FTP**
  Les paramètres suivants sont utilisés si la destination du fichier de sauvegarde est configurée sur **FTP**.
- **Adresse IP du serveur**
  Adresse, y compris le chemin du fichier, du serveur FTP.
- **Port**
  Port FTP du serveur. La valeur normale par défaut est le port 21.
- **Nom d'utilisateur** / **Mot de passe**
  Nom d'utilisateur et mot de passe pour accéder au fichier sur le serveur FTP précisé.
- **Sauvegarder**
  Ce bouton permet de lancer une sauvegarde à l'aide des paramètres ci-dessus.

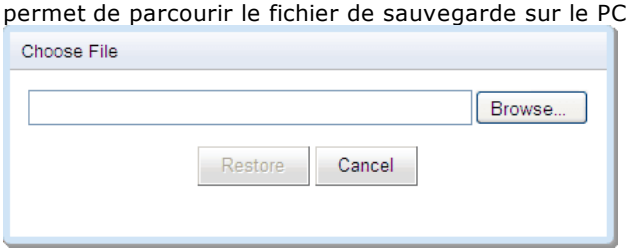
4.4.2 Restauration

Ce menu permet de sélectionner un fichier de sauvegarde différent pour ensuite l'utiliser dans le cadre d'une restauration. Avant de lancer la restauration, une sauvegarde de la configuration actuelle est effectuée et stockée dans le **Dossier de sauvegarde** pour l'utiliser avec la commande **Annuler la dernière restauration** 97. La restauration est uniquement prise en charge à partir d'une sauvegarde de la même version de one-X Portal for IP Office.



- **Restaurer à partir de**
  Ce paramètre permet de sélectionner le point de départ du fichier de sauvegarde précédent.
- **Serveur local**
  Si cette option est sélectionnée, le fichier de sauvegarde pour la restauration est sélectionné dans le **Dossier de sauvegarde**.
- **FTP**
  Si cette option est sélectionnée, le fichier de sauvegarde pour la restauration est sélectionné à partir de l'adresse du serveur FTP en question.
- **Lecteur Local**
  Si cette option est sélectionnée, le fichier de sauvegarde pour la restauration est sélectionné à l'aide d'un menu de navigation de fichiers pour trouver un fichier sur le PC.
- **Paramètres FTP**
  Les paramètres suivants sont utilisés si la destination du fichier de sauvegarde est configurée sur **FTP**.
- **Adresse IP du serveur**
  Adresse, y compris le chemin du fichier, du serveur FTP.
- **Port**
  Port FTP du serveur. La valeur normale par défaut est le port 21.
- **Nom d'utilisateur** / **Mot de passe**
  Nom d'utilisateur et mot de passe pour accéder au fichier sur le serveur FTP précisé.
- **Affichage des sauvegardes disponibles**
  Ce bouton est indiqué quand l'option **Restaurer à partir de** est configurée sur le **Serveur local** ou un **FTP**. Si vous cliquez dessus, une liste des fichiers de sauvegarde disponibles à l'emplacement indiqué apparaît. Sélectionnez un fichier et cliquez sur **Restaurer** pour commencer le processus de restauration.

- **Choisir un fichier**
  Ce bouton est disponible quand l'option **Restaurer à partir de** est configurée sur le **Lecteur local**. Il vous permet de parcourir le fichier de sauvegarde sur le PC.



Index

4

4560 89

A

À propos de 12
Accessible 38
Activer
  Gadget externe 65
Administrateur
  Aide 50
  Nom 9
Affichage
  Conférence 49
  État des composants 15
  Événements récents majeurs 17
Afficher
  Fournisseurs 19
Aide 12
  À propos de 50
  Aide 50
  Assistance technique Avaya 50
Ajout
  gadget 64
  IP Office 54
  LDAP 68
  Utilisateur 66
Annuaire
  Exportation 25
  Nouvelle synchronisation 43, 71
Annuaire personnel 66
Annuaire système 12
  Exportation 25
  Nouvelle synchronisation 43, 71
  Recherche dans le répertoire 45, 71
Apache
  Chainsaw 38, 89
Archive
  Sessions MI 76
Assistance technique Avaya 12
Attribution
  Fournisseur de messagerie vocale 23
  Fournisseur LDAP 22
  Fournisseurs 19
  IP Office 54, 56
  IP Office (CSTA) 20
  IP Office (Répertoire) 21

B

Base de données
  Vérification 39
  Vérification de l'état de santé 39
Base de recherche 68
Blocage du client 34

C

Calendrier 27, 81
Chainsaw 38, 89
Clients bloqués 34
Conférence 49
Conférence audio 49
Conférence Web 49
Configuration 12
  CSV 25
  Exportation 25
  Fournisseurs 19
  MI 77
  Modification en bloc 66
  Personnalisation 25
  Présence 77
  Utilisateurs 24
Configuration des journaux 89
Connexion 9
  Échec 17
Connexion autorisée à tous les utilisateurs. 77
Consignation
  Afficheur 12
  Configuration 12
Consultation des journaux à distance 89
Contrôler 49
CSTA 20
CSV 12, 25

D

Déconnexion 9
Déconnexion automatique 9
Déconnexion en cas d'inactivité. 77
Déconnexion immédiate 9
Démarrage du service 52
Désinstallation 74
Diagnostics 12
  Configuration des journaux 36, 89
  Connexions 39
  Connexions IP Office 39
  Intégrité de la base de données 39
  Itinéraires réseau 38
  Visionneuse de journaux 38, 89

E

Échecs de connexion 17
Echo 38
Emplacements de parcage 66
Environnement 12
État
  Composant 15
  MI 79
  Présence 79
État de santé 39
État des composants 12, 15
État d'intégrité 12
  Environnement 18
  État des composants 15
  Événements récents majeurs 17
  Sessions actives 18
Événements 17
Événements récents 17
Événements récents majeurs 12, 17
Exceptions 66
Exceptions à NPD 66
Exchange 27, 81
Exportation
  Gadgets 47, 63
Exportation de la configuration 25
exportDirectoryEntry.csv 25
exportUser.csv 25

F

Fichiers journaux 36
Fichiers journaux tournants 36
Format Log4j 89
Fournisseur 12
  Affichage 19
  Attribution 19

Fournisseur 12
CSTA (IP Office) 20
DSML (IP Office) 21
DSML (LDAP) 22
Messagerie vocale 23
Répertoire (DSML IP Office) 21
Répertoire (DSML LDAP) 22
Fournisseur CSTA (IP Office) 20
Fournisseur DSML (IP Office) 21
Fournisseur DSML (LDAP) 22

G

Gadget
Activer 65
Désactiver 65
Exportation 47, 63
Importer 61
Modification 64
Suppression 65
URL 60
Gadgets
Liste des gadgets externes 46

I

Ignorer la session administrateur 9
Importer
Gadgets 61
Inaccessible 38
Intégration des répertoires 12
Annuaire système 45, 71
LDAP 43, 70
Synchronisation des répertoires 43, 71
Intégrité de la base de données 12
IP Office
Connexions 12
Fournisseur CSTA 20
Fournisseur de répertoire 21
Itinéraires réseau 12, 38

J

Java Web Start 89
Journal des appels 66
Journalisation 89
Afficheur 89
Cibles 36
Niveau 36

L

LDAP 70
Attribution 68
Fournisseur 22
Recherche dans le répertoire 12, 43, 70

M

Mappage des champs 22, 68
Messagerie vocale
Fournisseur 23
Messages 66
Messages vocaux 66
MI
Archivage 76
Configuration 77
État 79
Rechercher des sessions 48, 80
Mise à niveau 72
Modification
Gadget 64
Modification en bloc 66
Paramètres IP Office 56
Paramètres utilisateur 24, 66
Modification en bloc 24, 66
Utilisateur 66
Mot de passe 9

N

Niveau de consignation principal 36
Nom de domaine
Nom de domaine XMPP 77
Nom de domaine XMPP 77
Nom unique de base 68
Nouvelle synchronisation 43, 71
Nouvelle synchronisation forcée 43, 71

P

Panneau de configuration 74
Paramètres
Modification en bloc 66
Participants 49
Personnalisation 25
PING 38
Port
4560 89
7 38
Port TCP 7 38
Présence 66
Configuration 77
État 79
Exchange 27, 81

R

Raccourcis 66
Raccourcis clavier 66
Récepteur de socket 36, 89
Recherche
Sessions MI 48, 80
Recherche dans le répertoire
Annuaire système 45, 71
LDAP 43, 70
Rechercher
Annuaire système 45, 71
LDAP 43, 70
Redémarrage du service 52
Réinitialiser le nombre de sessions 9
Répertoire (DSML IP Office) 21
Répertoire (DSML LDAP) 22
Répertoire externe
Rechercher 43, 70
Rétrogradation 73
Routes 38

S

Sauvegardes 12
Serveur
Informations 18
Version 18
Service
Redémarrage 52
Sessions 18
Sessions actives 12, 18
Suppression
Gadget 65
IP Office 56
one-X Portal for IP Office 74
Utilisateur 66
Supprimer

Supprimer
IP Office 56
Utilisateur 66
Synchronisation 43, 71
Synchronisation des répertoires 12
T
Temporisation d'inactivité. 77
Test
Annuaire système 45, 71
Connexion IP Office 39
Itinéraire réseau 38
Répertoire externe 43, 70
Répertoire LDAP 43, 70
U
Utilisateur
Aide 50
Ajout 66
Exportation 25
Modification des paramètres 66
Modification en bloc 66
Supprimer 66
Validation des données 40
Utilisateurs 12
Actifs 18
Affichage 24
Modification des paramètres 24
Nouvelle synchronisation 43, 71
V
Validation des données 40
Version 18