Bulletin Technique	Alcatel-Lucent OmniPCX Office RCE

TC1143 ed.11

Toutes les Releases

RECOMMANDATIONS DE SECURITE POUR L'OMNIPCX OFFICE RCE

Ce document fournit aux clients d'Alcatel-Lucent Enterprise les recommandations pour configurer une sécurité optimale pour se protéger des utilisations ou des accès non autorisés aux fonctions de l'OmniPCX Office RCE.

Historique

Edition 11: 28 novembre 2014 réécriture du chapitre Sécurité réseau, ajout des fonctions R10.0

Sommaire

1 Introduction

Cette communication technique fournit aux clients les recommandations d'Alcatel-Lucent Enterprise afin de configurer une sécurité optimale lors de l'installation des systèmes OmniPCX Office RCE.

L'OmniPCX Office RCE fournit de nombreuses fonctionnalités qui peuvent être accessibles de différents endroits, sites distants ou Internet inclus.

Des mesures de sécurités et de contrôles fournis par notre système permettent l'accès et l'utilisation de ces fonctions tout en optimisant la sécurité de la solution. Comme on ne peut pas complètement exclure qu'un système de télécommunication soit la cible d'utilisations non autorisées, il est très important que l'installateur et l'utilisateur/administrateur du système prêtent une attention particulière à la gestion du système ainsi qu'aux recommandations de sécurité d'Alcatel-Lucent Enterprise pour réduire efficacement ce type de risque.

Il est de la responsabilité de l'installateur de soigneusement informer l'utilisateur/administrateur des fonctions de sécurité de l'OmniPCX Office RCE et de s'assurer qu'il ait une bonne compréhension des vulnérabilités du système si les recommandations d'Alcatel-Lucent Enterprise ne sont pas rigoureusement et constamment suivies.

L'installateur doit également discuter avec l'utilisateur/administrateur du système, du niveau de sécurité qu'il attend, l'informer en conséquence et mettre en œuvre les configurations appropriées pour personnaliser au mieux le système tout en répondant à des niveaux de sécurité tels que, mais pas uniquement, ne pas activer le service Assistant Personnel ou la configuration à distance d'un renvoi (depuis R700) si ces fonctions ne sont pas demandées ou prévues par l'utilisateur/administrateur du système.

2 Contrôle d'accès : politiques de mot de passe

Il est essentiel d'examiner la configuration de sécurité lors de l'exposition de services de l'OmniPCX Office RCE à des accès externes, comme par exemple via Internet. L'accès aux services utilisateurs de l'OmniPCX Office RCE est protégé par un mot de passe défini et géré par l'utilisateur conformément à la politique énoncée ci-dessous.

Ce mot de passe unique autorise l'accès aux fonctions suivantes :

- configuration de la boîte vocale,
- configuration de l'assistant personnel,
- gestion du mot de passe,
- configuration du mode nomadic,
- activation d'un renvoi,
- substitution distante,
- accès à la boite vocale,
- connexion de PIMphony avec l'OmniPCX Office RCE,
- verrouillage du poste,
- My IC Web for Office,
- My IC Mobile / OpenTouch Conversation (OTCV).

2.1 Gestion du mot de passe usager

La création et la sécurité du mot de passe relèvent de la responsabilité de l'utilisateur/administrateur du système. L'installateur doit s'assurer que l'utilisateur/administrateur du système ait connaissance et comprenne que : (a) la mise en œuvre, le respect strict et constant d'une politique de gestion de mot de passe, au moins conforme avec les recommandations énoncées dans la présente communication technique, est la clé pour protéger le système d'une utilisation non autorisée et (b) que toute personne accédant à l'assistant personnel ou à la substitution à distance (DISA Transit) en utilisant un mot de passe correct est implicitement un utilisateur autorisé à utiliser ce mot de passe. Le système OmniPCX Office RCE demande le changement du mot de passe par défaut pour chaque messagerie vocale donnée lorsque cette messagerie vocale est initialisée.

Les recommandations élémentaires d'Alcatel-Lucent en matière de sécurité sont les suivantes :

- Configurer des mots de passe sécurisés à la place des mots de passe par défaut si vous utilisez des applications directement connectées à votre OmniPCX Office RCE comme par exemple la boîte vocale, l'assistant personnel ou connectées par le WAN comme My IC Mobile, PIMphony, etc...
- obliger les utilisateurs à changer régulièrement leur mot de passe.
- proscrire l'usage de mots de passe dits triviaux, tels que 1234, 0000, 1111, etc...
- veiller à ce que les personnes ne se communiquent pas les mots de passe entre elles (autres personnes/collègues, etc ...).
- veiller à ce que les personnes verrouillent au besoin leur poste en dehors des périodes d'utilisation (vacances, week-ends, etc...).

Important

Les mots de passe dits triviaux sont contrôlés par le système à partir des versions R410/065.001, R510/059.001, R610/047.001, R710/052.007, R800/030.002, R810/045.003, R820/026.007, R900/033.002 et R910/021.001.
A partir des versions R800/043.001 et R810/047.001 la liste des mots de passe dits triviaux a été étendue.
Lors de la saisie d'un mot de passe considéré par l'OmniPCX Office comme étant trivial, le message « Saisie non valide » est diffusé.

Important

Depuis les versions R820/026.007, R900/033.002 et R910/021.001 le système peut être configuré pour utiliser des mots de passe usager à 6 chiffres. Un nouveau système démarre automatique avec des mots de passe à 6 chiffres alors qu'un système mis à jour vers une des ces versions conserve les mots de passe à 4 chiffres mais dans ce cas, à chaque connexion d'OMC, un message recommandant de passer les mots de passe à 6 chiffres sera affiché.

Note

Après un swap avec data-saving, d'une version antérieure à une de celle mentionnée ci-dessus, si des mots de passe triviaux étaient utilisés ils seront restaurés dans le système. Dans ce cas il est de la responsabilité de l'utilisateur, l'administrateur ou de l'installateur de vérifier que nos recommandations de sécurités sont appliquées.

Note

Depuis la version R9.1 une nouvelle fonction du système permet de vérifier si des mots de passe triviaux sont utilisés. Une fonction supplémentaire permet de remettre à la valeur par défaut tous les mots de passe des utilisateurs ayant des mots de passe triviaux (voir la Documentation Expert pour plus de détails).

2.2 Gestion des mots de passe système

Des règles similaires doivent être appliquées pour les différents mots de passe utilisés par OMC pour se connecter au système. Il est recommandé de modifier le mot de passe par défaut ***Installateur*** pour OMC Expert, ***Administrateur*** pour OMC EasyPlus et ***Opérateur*** pour OMC Easy. Ces mots de passe sont également utilisés pour les connexions par DHM-Poste.

Les recommandations élémentaires d'Alcatel-Lucent en matière de sécurité sont les suivantes :

- changer régulièrement leur mot de passe.
- définir et appliquer une stratégie d'entreprise rigoureuse vis-à-vis des usagers internes.
- proscrire l'usage de mots de passe dits triviaux, tels que 12345678, 11111111, 00000000, etc...
- ne choisissez pas un mot du langage de tous les jours. Une intrusion peut être réalisée à l'aide de logiciels spécialisés utilisant des dictionnaires de mots.
- ne choisissez pas un mot en relation avec vous-même : le nom de votre société, votre nom, le nom de jeune fille de votre femme, le nom de vos enfants, de votre chien, de votre loisir favori, etc…
- prenez un mot de passe différent par mode de connexion.
- votre mot de passe est personnel et doit rester confidentiel, ne le divulguez jamais à personne.
- un mot de passe ne doit jamais être écrit quelque part. La première chose que fait une personne malveillante, est de fouiller dans vos affaires.

Attention

Les mêmes règles doivent être appliquées au mot de passe de la session ***Téléchargement de logiciel***. Le mot de passe par défaut est identique à celui par défaut de la session Installateur. Mais la session Téléchargement possède un mot de passe spécifique qui peut être modifié avec OMC Expert.

Note

Un niveau supplémentaire de sécurité peut être réalisé en activant les fonctions « Rappel / Appelants Autorisés » dans le menu OMC « Gestion et Contrôle Réseau ». Ceci permet d'avoir le contrôle total sur qui est autorisé à se connecter au système (pour plus de détails voir la Documentation Expert).

Depuis la R9.1 tous les mots de passe de gestion du système (à l'exception du mot de passe Opérateur) doivent respecter de nouvelles règles (contrôlées par le système). Il faut au minimum:

- une longueur fixe de 8 caractères,
- une lettre majuscule (A-Z),
- une lettre minuscule (a-z),
- un chiffre (0-9),
- pas de caractères spéciaux.

Depuis la R10.0 (première version) le mot de passe Operateur doit respecter de nouvelles règles (contrôlées par le système). Il faut au minimum:

- une longueur fixe de 8 caractères,
- au moins un chiffre (par exemple "HelloYou" sera refusé, "Hello123" est accepté),
- au moins deux caractères différents (par exemple "11111111", "aaaaaaaa" seront refusés),
- pas de suite de caractères montante ou descendante (par exemple "12345678", "abcdefgh" seront refusés),
- pas de caractères spéciaux.

Note

Depuis la version R9.1 une nouvelle fonction du système permet de vérifier si des mots de passe par défaut ou triviaux sont utilisés (voir la Documentation Expert pour plus de détails).

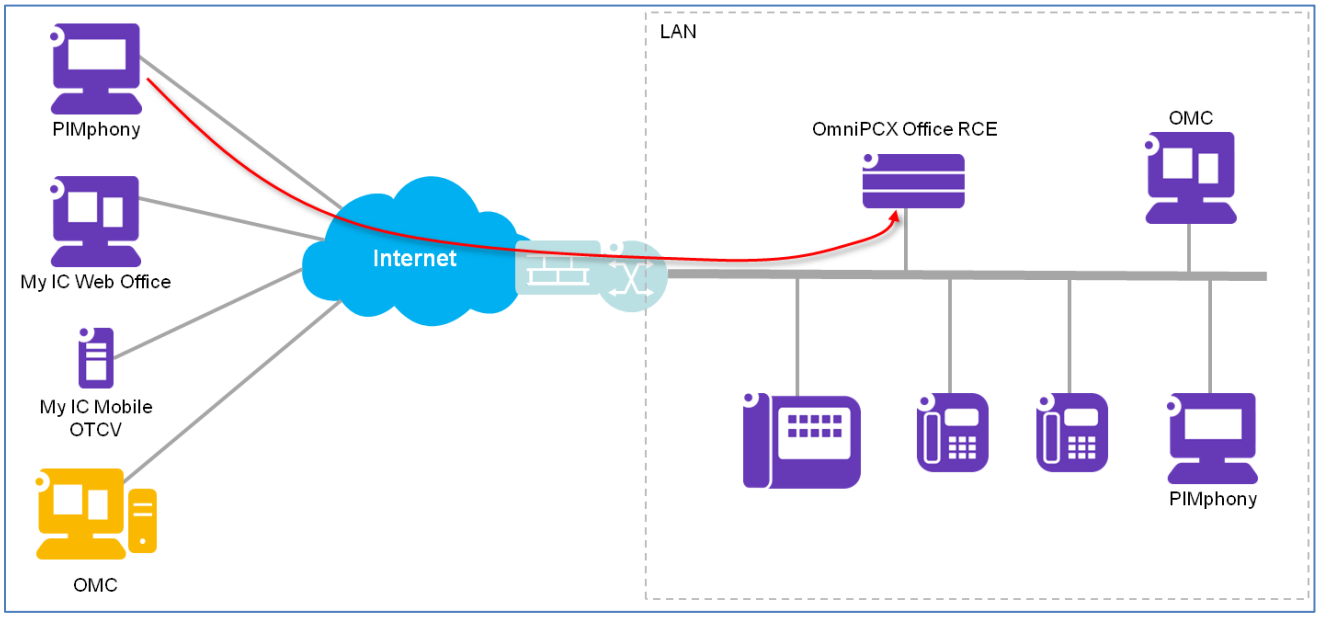
Important

Depuis la version R9.0 il faut impérativement fournir soit le numéro de série de la CPU ainsi que l'adresse MAC soit directement le CPU ID lors d'une demande (service request) de remise à la valeur par défaut du mot de passe installateur.

3 Sécurité réseau: configuration de l'accès à distance

3.1 Sécurité de l'accès Internet

Les équipements connectés au LAN (Local Area Networks) ont habituellement accès à Internet au travers d'un routeur ou d'un périphérique d'accès Internet. De nos jours, cet équipement propose en règle générale une fonctionnalité pare-feu permettant la protection du LAN contre les menaces extérieures.
L'OmniPCX Office RCE n'est pas directement connecté à Internet mais est connecté au LAN. L'accès à distance à l'OmniPCX Office RCE à partir d'Internet se fait habituellement au travers d'un périphérique d'accès Internet possédant une fonction pare-feu vers le LAN. L'accès à distance peut être nécessaire à certaines applications des utilisateurs (My IC Web for Office, My IC Mobile/OTCV, and PIMphony) ou aux applications de gestion (OMC, Web-Based Tool).



En conséquence, il est important d'appliquer des mesures de sécurité appropriées dans la configuration du pare-feu/périphérique d'accès Internet afin d'assurer une connexion à distance sécurisée vers l'OmniPCX Office RCE.

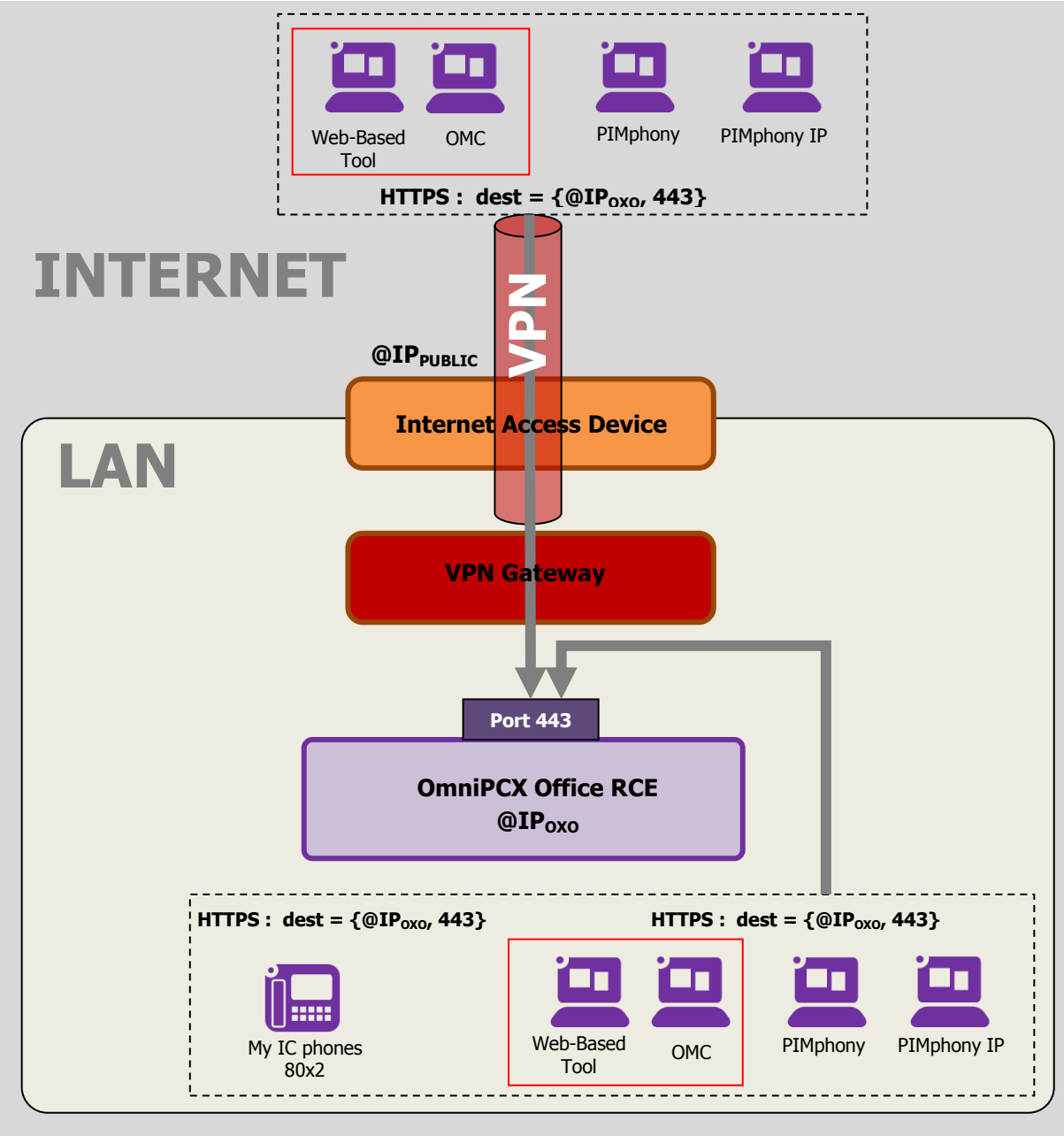
L'accès à distance ne doit être activé que si nécessaire. Si cet accès à distance est nécessaire, il faut appliquer avec attention les recommandations des sections suivantes en rapport avec la version de votre système.

3.2 Accès à distance à l'OmniPCX Office RCE avant R820

Avant la R820, une connexion VPN est obligatoire pour une connexion à distance d'une application à partir d'Internet aux services de l'OmniPCX Office RCE dans le LAN du client.

Ni l'OmniPCX Office RCE, ni les applications des utilisateurs finaux ne fournissent un service de VPN. Un logiciel/équipement supplémentaire est nécessaire pour gérer la connexion VPN.

La sécurité de cette solution de VPN est sous la responsabilité de son propriétaire.



3.3 Accès à distance à l'OmniPCX Office RCE pour R820 et releases supérieures

Pour la R820 et les versions supérieures, les accès à distance à partir d'Internet sont possibles en respectant les principes de sécurité suivants :
Pour rappel, l'OmniPCX Office RCE n'est pas directement connecté à Internet mais est connecté au LAN. Le système fait la différence entre les connexions venant d'Internet de celles venant du LAN en se basant sur le port de destination de l'OmniPCX Office RCE :

- Les ports 443 et 10443 sont dédiés aux connexions venant du LAN,
- Le port 50443 est dédié aux connexions venant d'Internet et permet d'appliquer une politique de contrôle d'accès.

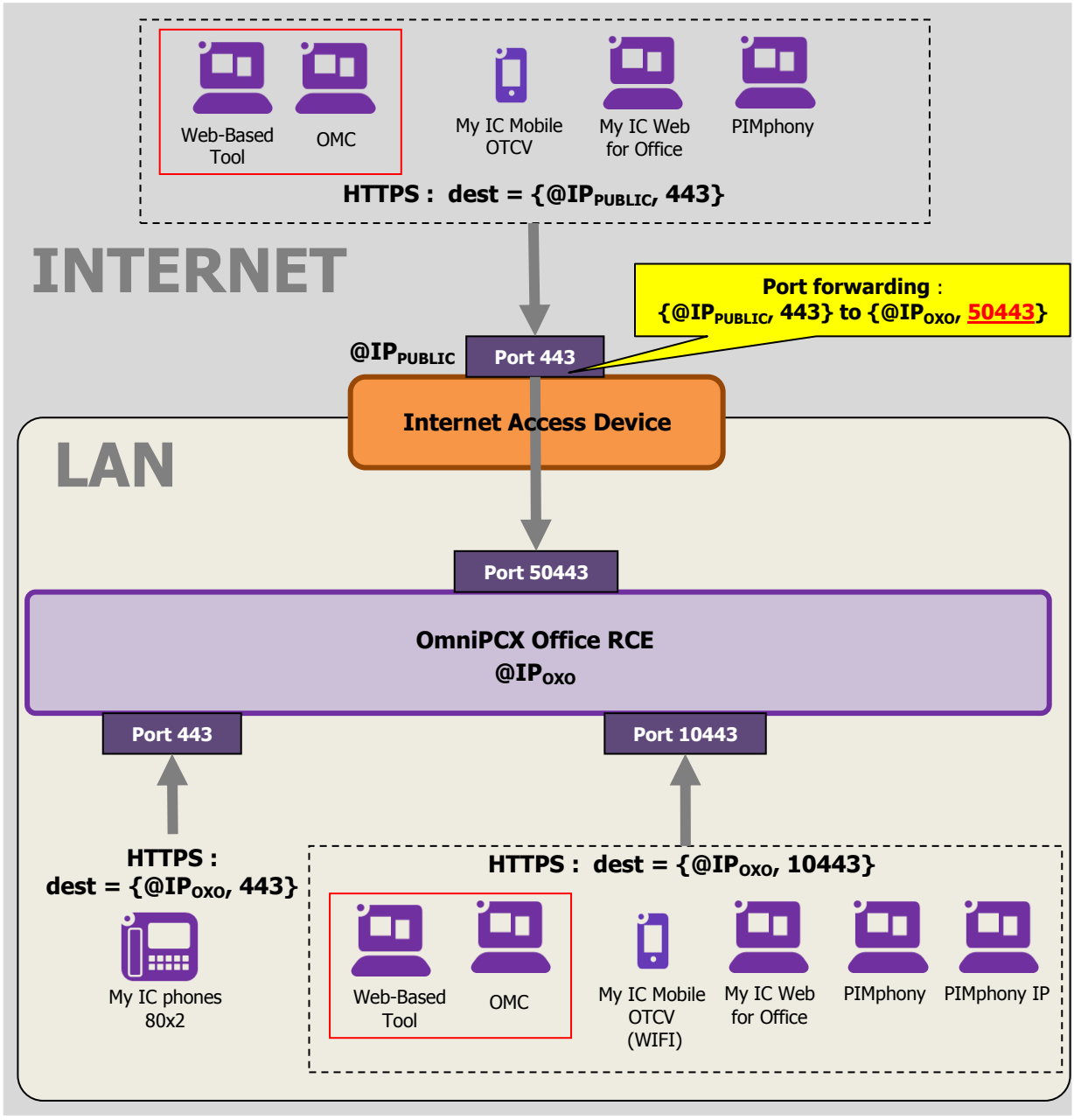


Fig. 1 : OmniPCX Office RCE R820

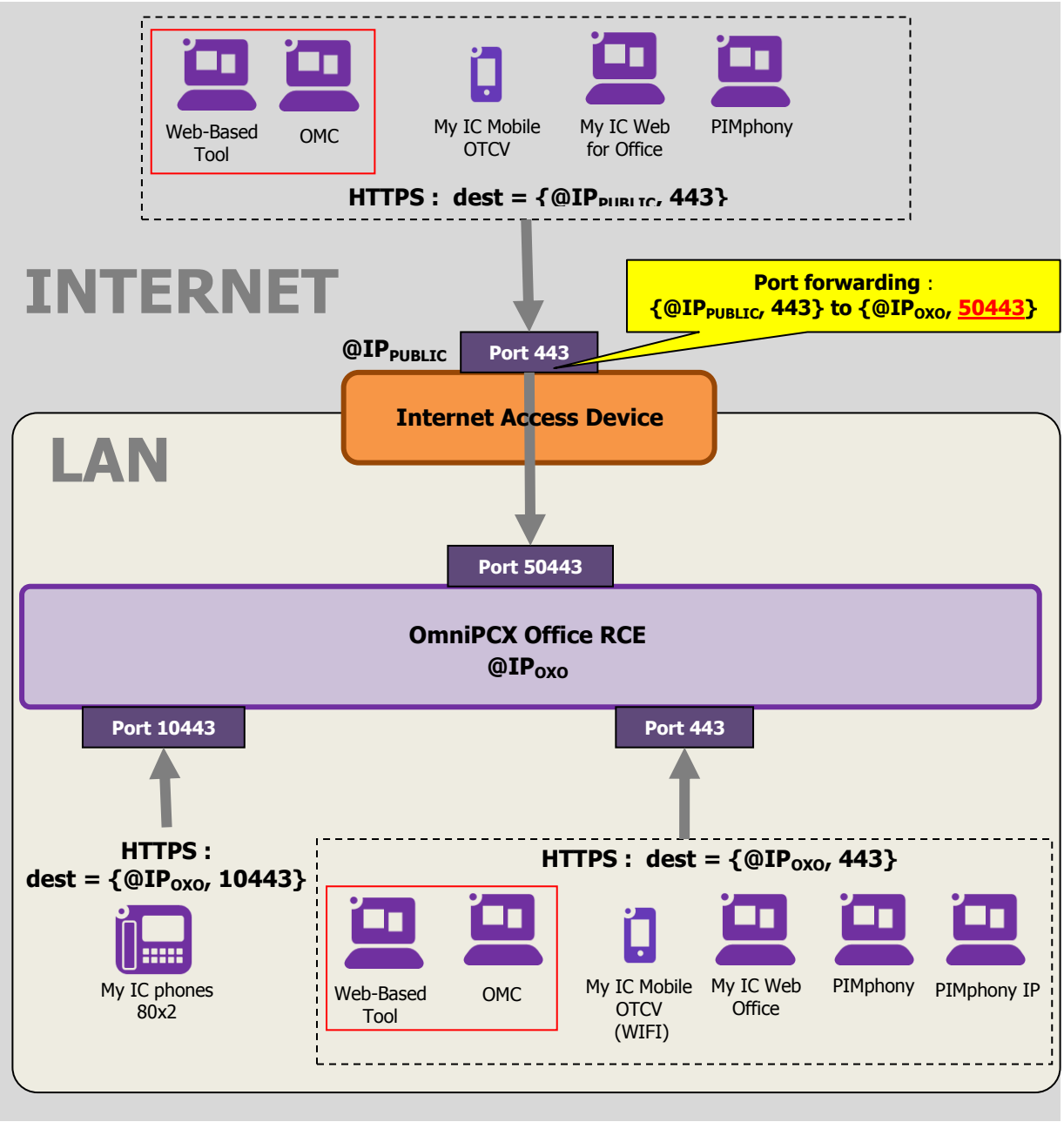


Fig. 2 : OmniPCX Office RCE R900 et releases supérieures

Toute connexion à distance à partir d'Internet arrive sur l'interface publique du périphérique de connexion à Internet qui redirige ce trafic vers l'OmniPCX Office RCE sur le LAN.

Les applications qui se connectent à partir d'Internet à l'OmniPCX Office RCE doivent utiliser le protocole https. Le port de destination utilisé par défaut par les applications est le port standard https 443. Dans certains cas, un autre port doit être utilisé : voir le chapitre suivant pour plus d'explication.

Une redirection de port doit être configurée dans le périphérique d'accès à Internet afin de rediriger le trafic entrant sur le port public 443 vers le port 50443 de l'OmniPCX Office RCE.

Redirection {@IP$_{PUBLIC}$, port 443} vers {@IP$_{OXO}$, port **50443**}

Attention

Règles de sécurité :

- Le port de destination des accès à distance à partir d'Internet dirigés vers l'OmniPCX Office RCE doit toujours être 50443
- Ne jamais rediriger du trafic venant d'Internet vers un autre port que le port 50443 de l'OmniPCX Office RCE, exception faite pour le besoin explicite de l'utilisation d'un IP trunk public
- Ne jamais rediriger du trafic venant d'Internet vers les ports 443 ou 10443 de l'OmniPCX Office RCE.

Note

Les terminaux My IC Phone utilisent sur le LAN le port 443 de l'OmniPCX Office RCE R820. Et utilisent le port 10443 de l'OmniPCX Office RCE pour les releases supérieures à R820.

Note

Une connexion par VPN reste toujours possible pour ce type de topologie d'accès à distance des applications (voir chapitre 3.2).

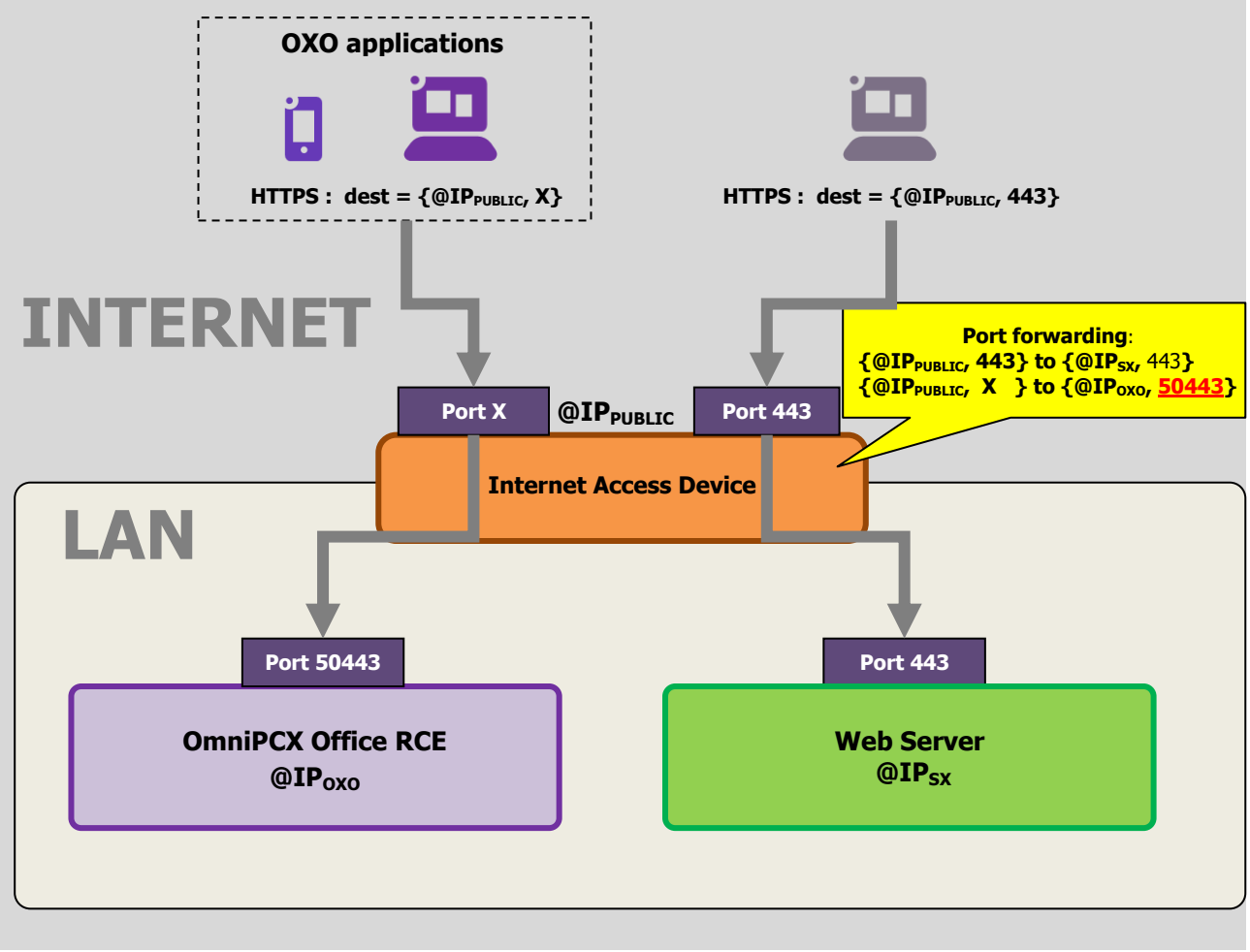
Important

Dans le cas d'une connexion à distance de PIMphony IP, seule la solution basée sur un VPN est supportée.

3.4 Accès à distance à l'OmniPCX Office RCE lorsque le port publique 443 est déjà utilisé

On part du principe qu'une seule adresse IP publique est assignée au périphérique d'accès à Internet.
Si en plus de l'OmniPCX Office RCE un autre serveur HTTPS (per exemple serveur web) est connecté au LAN, alors différents ports doivent être utilisés au niveau du périphérique d'accès à Internet pour joindre chaque serveur à partir d'Internet. Un des ports peut rester le port standard https 443. L'autre port peut être n'importe quel autre port non utilisé sur le périphérique d'accès à Internet.
Pour rappel, le port de destination des applications se connectant à l'OmniPCX Office RCE à partir d'Internet n'est pas un port de l'OmniPCX Office RCE mais un port de l'interface publique du périphérique d'accès à Internet. Tout trafic reçu sur le port public du périphérique d'accès à Internet est redirigé vers le port 50443 de l'OmniPCX Office RCE sur le LAN.

Exemple:



Configuration générique:

- Pour se connecter à l'OmniPCX Office RCE à partir d'Internet, utilisez l'adresse de destination {@IP_{PUBLIC}, port X}
- Pour se connecter au server web à partir d'Internet, utilisez l'adresse de destination {@IP_{PUBLIC}, port 443}

Configuration correspondante de la redirection de ports dans le périphérique d'accès à Internet :

- Redirigez {@IP_{PUBLIC}, port X} vers {@IP_{OXO}, port 50443}
- Redirigez {@IP_{PUBLIC}, port 443} vers {@IPsx, port 443}

Attention

Règles de sécurité :

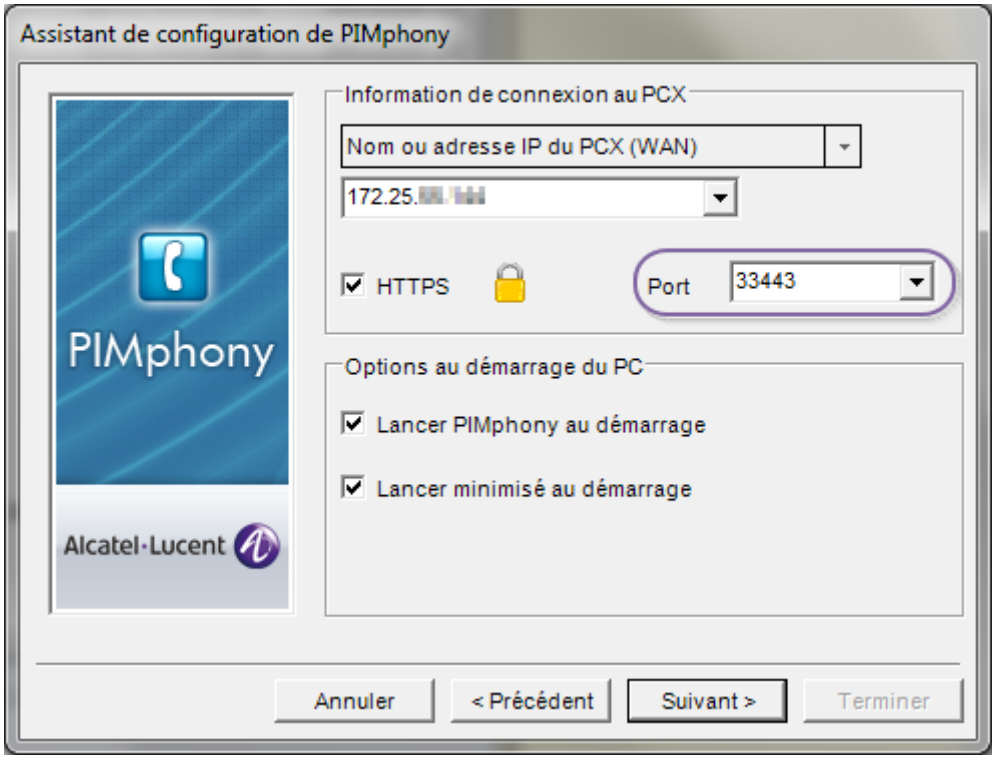
- Le port de destination des accès à distance à partir d'Internet dirigés vers l'OmniPCX Office RCE doit toujours être 50443
- Ne jamais rediriger du trafic venant d'Internet vers un autre port que le port 50443 de l'OmniPCX Office RCE, exception faite pour le besoin explicite de l'utilisation d'un IP trunk public
- Ne jamais rediriger du trafic venant d'Internet vers les ports 443 ou 10443 de l'OmniPCX Office RCE.

3.4.1 Configuration du port de connexion des applications pour les utilisateurs

Si un port différent du port standard https 443 est utilisé comme port de destination publique sur le périphérique de connexion à Internet, alors celui-ci doit être configuré comme nouveau port de destination pour chaque application des utilisateurs.
L'autre port peut être n'importe quel autre port non utilisé sur le périphérique d'accès à Internet. Le même port peut être utilisé pour toutes les applications.

3.4.1.1 PIMphony

Pour PIMphony (PIMphony associé à un poste physique de l'OmniPCX Office RCE) le port de destination utilisé pour l'accès à distance doit être défini dans l'assistant de configuration :



3.4.1.2 My IC Mobile / OpenTouch Conversation (OTCV)

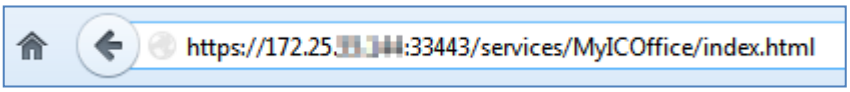
L'URL publique utilisée par l'application pour se connecter à partir d'Tnternet est définie dans son fichier de configuration. Par défaut le port de destination est le port 443. Pour utiliser un port différent if faut configurer celui-ci avec l'adresse remarquable "**ExtHttpsPo**".

Par exemple si on veut utiliser le port 33443, ExtHttpsPo doit être positionné à la valeur 82 A3 (Hex).

L'URL publique ou l'adresse IP sont définies dans OMC \ Matériels et Limites → Configuration LAN → Adresse IP du routeur/Nom de Domaine

3.4.1.3 My IC Web for Office

My IC Web for Office est une application web: le port de destination est défini dans le navigateur.

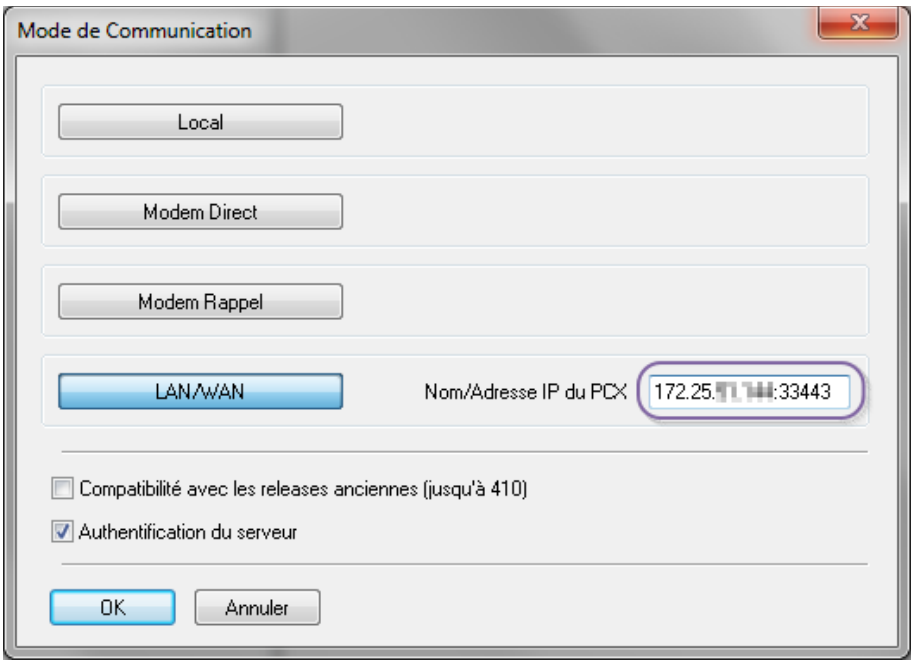


3.4.2 Configuration du port de connexion des applications de gestion

Si un port différent du port standard https 443 est utilisé comme port de destination publique sur le périphérique de connexion à Internet, alors celui-ci doit être configuré comme nouveau port de destination pour chaque application de gestion.
L'autre port peut être n'importe quel autre port non utilisé sur le périphérique d'accès à Internet. Le même port peut être utilisé pour toutes les applications.

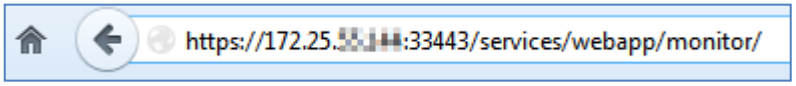
3.4.2.1 OMC

Par défaut le port de destination est le port 443.
Le port de destination peut être défini dans le champ Nom/Adresse IP du PCX dans la fenêtre de connexion d'OMC :



3.4.2.2 Web-Based Tool

Le Web-Based Tool est une application web: le port de destination est défini dans le navigateur.



4 Paramètres de configuration système

L'OmniPCX Office propose de nombreux paramètres de configuration permettant d'optimiser le niveau de sécurité.

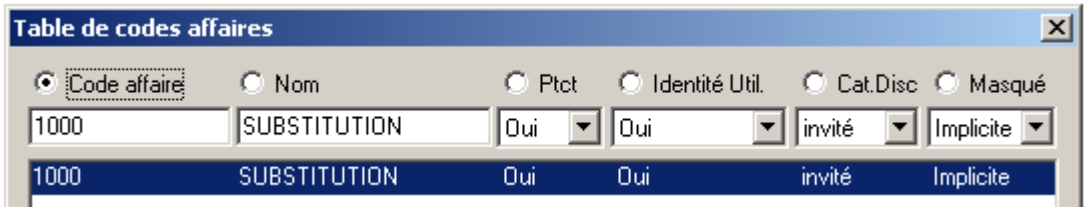
4.1 Toutes les Releases – Table des codes affaires

Attention

Par défaut, les paramètres contrôlant l'aboutement externe/externe de l'assistant personnel sont la matrice/table de discrimination et catégories de service du poste de l'usager.

Cependant, selon la configuration de la « Table de codes affaires » (voir ci-après), il est possible d'appliquer un type de contrôle différent.

Configuration par défaut : la table des codes affaires contient une ou plusieurs entrées de ce type



Dans ce cas, contrôle par matrice/table de discrimination et catégories de service du poste de l'usager

- Configuration modifiée :

Si dans la table codes affaires, toutes les entrées avec catégorie de discrimination « Invité » ont été supprimées, **le contrôle d'aboutement s'effectue avec les paramètres de discrimination (matrice et table) des équipements de messagerie vocale.**

4.2 R110, R210 et release supérieure – configuration usager et système

En désactivant les fonctions suivantes, il est possible d'empêcher un appel entrant d'effectuer un break-out par transfert manuel ou suite à un renvoi.

- Par poste / Service Cat – Aboutement Entrant/Sortant
- Particularités système / Partie 2 – Transfert Ext/Ext
- Particularités système / Partie 2 – Transfert Ext/Ext par raccrochage
- Matrice et table de discrimination par poste (selon le mécanisme décrit plus haut)
- Aboutement

4.3 De R310 à la Release courante – Catégorie de services usager "Configuration distante"

La "configuration distante" est configurable poste par poste dans OMC – Liste des Postes – Catégorie de service – Partie 2 – "Configuration distante". Cette fonction désactive le menu options personnelles (option 9) de la boite vocale.

Important

Cette Fonction est disponible depuis la R310/060.001, R410/065.001, R510/059.001, R610/047.001, R710/069.001, R800/030.00, R810/045.003, R820/026.007, R900/033.002 et R910/021.001. Par défaut, cette fonction est désactivée et l'option 9 (options personnelles) n'est pas disponible.

Note

Il faut obligatoirement utiliser l'OMC 800/21.1b ou une version supérieure. Cette fonction n'est pas disponible avec l'OMC 711.

Attention

Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.4 De R310 à la Release courante – Assistant Personnel

L'adresse remarquable nommée **PerAssAlwd** a été introduite en R310/055.001, R410/056.001, R510/035.001, R610/012.001 ainsi que dans la première version des releases R7.0, R7.1, R8.0, R8.1, R8.2, R9.0 et R9.1.
Cette adresse permet d'activer/désactiver la fonction Assistant Personnel au niveau du système.

Important

Depuis les versions R410/064.001, R510/058.001, R610/033.001, R700/026.001, R710/022.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 et R910/021.001 la valeur par défaut de cette adresse remarquable est **00H** (Assistant personnel désactivé par défaut).

Rappel

En R310 la valeur par défaut de cette adresse remarquable est **01H** (Assistant personnel activé par défaut).

Note

Après un swap avec data saving, d'une version R6.x ou R7.x antérieure, vers une version R610/033.001 ou R710/022.001, il est nécessaire de réactiver la fonction "Assistant Personnel", si celle ci était préalablement utilisée par le client.

Attention

Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.5 De R310 à la Release courante – Nombre de tentatives d'accès à la messagerie

L'adresse remarquable nommée **VMUMaxTry** a été introduite en R310/060.001, R410/064.001, R510/058.001, R610/015.001 ainsi que dans la première version des releases R7.0, R7.1, R8.0, R8.1, R8.2, R9.0 et R9.1.
Cette adresse permet de spécifier le nombre de tentatives infructueuses d'accès à la messagerie vocale.

Important

Depuis les versions R310/060.001, R410/064.001, R510/058.001, R610/033.001, R700/026.001, R710/022.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 et R910/021.001 la valeur par défaut de cette adresse remarquable est **03H** (3 tentatives maximum).

Note

Le système ne transmet aucune information sur l'état de la boite vocale et l'accès à distance reste activé lorsque la boite vocale est verrouillée.
Si l'accès à distance est bloqué avant la troisième tentative (exemple : VMUMaxTry = 01), un appel malveillant pourra néanmoins faire le deuxième et troisième essai. Ces tentatives obtiendront l'annonce vocale "xxxx n'est pas votre mot de passe ", suivi de "au revoir" puis libération de l'appel.
Si la boite est verrouillée lors de la première tentative d'authentification, le même processus est appliqué (3 essais et libération de l'appel).

Attention

Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.6 De R710 à la Release courante – Configuration à distance d'un Renvoi

L'adresse remarquable nommée **DivRemCust** a été introduite en R710/028.001 ainsi que dans la première version de la R8.0, R8.1, R8.2, R9.0 et R9.1.
Cette adresse permet d'inhiber ou non la fonction "gestion du renvoi à distance".

Important

Depuis les versions R710/028.001, R800/030.002, R810/045.003, R820/026.007, R900/033.002 et R910/021.00 la valeur par défaut de cette adresse remarquable est **00H** (renvoi à distance désactivé par défaut, ce menu n'est pas disponible dans le menu de la boite vocale).

Attention

Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.7 De R510 à la Release courante – Demande de rappel à partir de la boîte vocale

L'adresse remarquable nommée **CallCorres** a été introduite en R510/064.001, R610/052.001, R710/097.001, R820/045.001, R900/037.001 ainsi que dans la première version de la release R910.
Cette adresse permet d'activer/désactiver la fonction de « rappel » (option 3) lors de la consultation de message laissé sur la boîte vocale de l'usager.

Important La valeur par défaut dépend du produit cible (pays) de l'OXO (00H fonction de rappel non disponible dans le menu de la boîte vocale, 01H fonction de rappel disponible dans le menu de la boîte vocale).

Attention Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.8 De R820 à la Release courante – Option utilisateur « accès WAN API »

L'option utilisateur « accès WAN API » a été introduite en R820 et dans toutes les versions supérieures.
Cette option permet d'autoriser ou d'interdire individuellement pour chaque utilisateur l'accès WAN aux requêtes venant du WAN qui sont redirigées sur le port 50443 de l'OmniPCX Office.
L'accès WAN peut être activé/désactivé dans OMC : Liste des postes/bornes – catégorie de service – partie 1 – « accès WAN API »

Important Autorisez l'accès WAN uniquement aux utilisateurs qui utilisent une application comme My IC Mobile, OTCV ou PIMphony en accès à distance. Il est fortement recommandé de configurer le router avec une redirection de port vers le port 50443 uniquement si vous autorisez l'accès WAN à l'OmniPCX Office et à ses utilisateurs.

Attention Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.9 De R820 à la Release courante – Interdire toutes connexions LAN/WAN

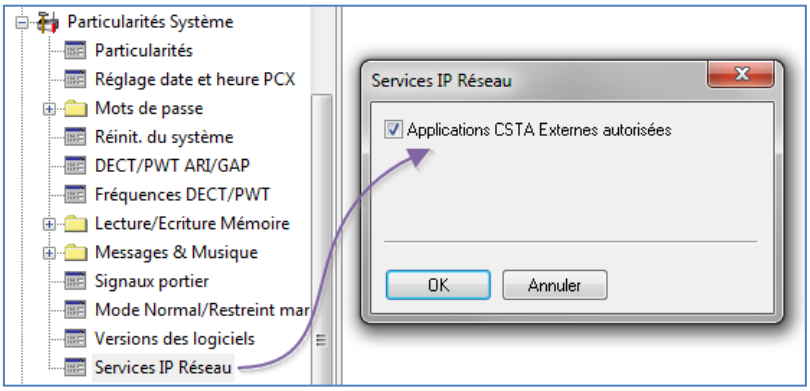
L'adresse remarquable nommée **ExtLnkClsd** a été introduite en R8.2 depuis la première version. Cette adresse permet d'ouvrir/de fermer toutes les connexions à l'OmniPCX Office venant du WAN et du LAN exception faite pour les connexions OMC qui sont toujours autorisées en respectant les recommandations du chapitre 3.

Important Par défaut toutes les connexions sont ouvertes, ExtLnkClsd = **00H**. Pour fermer ces connexions il faut positionner le flag à 01H; un redémarrage à chaud du système est nécessaire pour sa prise en compte.

Attention Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.10 De R820 à la Release courante – Contrôle d'accès des applications CSTA externes

Depuis la R820, l'accès pour les applications CSTA externes se connectant à l'OmniPCX Office RCE peut être autorisé ou interdit avec une option dans OMC.



Rappel

De R8.2 à R9.2 la valeur par défaut de l'option « Applications CSTA Externes autorisées » dépend du produit cible de l'OmniPCX Office RCE.

Important

A partir de R10.0, la valeur par défaut de l'option « Applications CSTA Externes autorisées » est désactivé pour tous les produits cible de l'OmniPCX Office RCE.

Note

Lors d'une migration d'une Release < R10.0 vers R10.0, la valeur définie dans la release antérieure est restaurée en R10.0. Par exemple, si l'accès aux applications CSTA externes se connectant à l'OmniPCX Office RCE était autorisé dans une release antérieure alors cette valeur sera restaurée en R10.0 après migration.

Attention

Il est fortement recommandé de mettre à jour les systèmes dans la dernière version de chaque release.

4.11 Depuis R10.0 – Gestion des certificats

La gestion des certificats a été améliorée en R10.0 et il est maintenant possible d'importer des certificats signés par une autorité externe, de créer une autorité de certification locale et de gérer un Trust Store.
Le Trust Store contient les autorités de certification les plus répandues et peut être étendu avec des certificats supplémentaire par l'installateur.

La sécurité a également été renforcée dans OMC grâce à un système de contrôle du certificat du système.

La gestion des certificats se fait à partir de l'interface du Web-Based Tool.
Pour plus de détails merci de se référer au chapitre 13 Sécurité / Gestion des certificats de la Documentation Expert.

5 Résumé des paramètres de sécurité

5.1 Adresses remarquables et options système

5.1.1 Options globales système

	VMUMaxTry	VMUMaxTry	PerAssAlwd	PerAssAlwd	DivRemcust	Callcorres
default value	20 (ancienne valeur)	03	01 (ancienne valeur)	00	00	dépendent du pays
R3.1	*non dispo.*[1]	310/060.001	310/055.001	*non dispo.*[1]	*non applic.*[2]	*non dispo.*[1]
R4.1	*non dispo.*[1]	410/064.001	410/056.001	410/064.001	*non applic.*[2]	*non dispo.*[1]
R5.1	*non dispo.*[1]	510/058.001	510/035.001	510/058.001	*non applic.*[2]	510/064.001
R6.1	610/015.003	610/033.001	610/012.001	610/031.001	*non applic.*[2]	610/052.001
R7.0	700/012.005	700/026.001	700/012.005	700/026.001	*en R710*	*en R710*
R7.1		710/022.001		710/022.001	710/028.001	710/097.001
R8.0		800/030.002		800/030.002	800/030.002	*en R820*
R8.1		810/045.003		810/045.003	810/045.003	*en R820*
R8.2		820/026.007		820/026.007	820/026.007	820/045.001
R9.0		900/033.002		900/033.002	900/033.002	900/037.001
R9.1		910/021.001		910/021.001	910/021.001	910/021.001
R9.2		toutes		toutes	toutes	toutes
R10.0		toutes		toutes	toutes	toutes

	ExtLnkClsd	Contrôle d'accès des applications CSTA externes
default value	Désactivé 00	dépendent du pays de R8.2 à R9.2 Désactivé en R10.0
R3.1	*non dispo.*[1]	*non dispo.*[1]
R4.1	*non dispo.*[1]	*non dispo.*[1]
R5.1	*non dispo.*[1]	*non dispo.*[1]
R6.1	*non dispo.*[1]	*non dispo.*[1]
R7.0	*non dispo.*[1]	*non dispo.*[1]
R7.1	*non dispo.*[1]	*non dispo.*[1]
R8.0	*in R820*	*non dispo.*[1]
R8.1	*in R820*	*non dispo.*[1]
R8.2	toutes	toutes
R9.0	toutes	toutes
R9.1	toutes	toutes
R9.2	toutes	toutes
R10.0	toutes	toutes

1: Non disponible signifie que l'adresse remarquable n'est pas disponible ou que la valeur par défaut indiquée n'est pas utilisée dans cette version.
2: Non applicable signifie que l'adresse remarquable n'est pas disponible dans cette version parce que la fonction sur laquelle elle s'applique n'existe pas dans cette version.
Version en bleu signifie que c'est la 1ère version de la release

5.1.2 Options usager

	Option usager « Configuration distante »	Option usager « accès WAN API »
default value	désactivé	désactivé
R3.1	310/060.001	*non dispo.*[1]
R4.1	410/065.001	*non dispo.*[1]
R5.1	510/059.001	*non dispo.*[1]
R6.1	610/047.001	*non dispo.*[1]
R7.0	*en R710*	*non dispo.*[1]
R7.1	710/069.001	*non dispo.*[1]
R8.0	800/030.002	*non dispo.*[1]
R8.1	810/045.003	*non dispo.*[1]
R8.2	820/026.007	820/019.001
R9.0	900/033.002	toutes
R9.1	910/021.001	toutes
R9.2	toutes	toutes
R10.0	toutes	toutes

1: Non disponible signifie que l'adresse remarquable n'est pas disponible ou que la valeur par défaut indiquée n'est pas utilisée dans cette version.
2: Non applicable signifie que l'adresse remarquable n'est pas disponible dans cette version parce que la fonction sur laquelle elle s'applique n'existe pas dans cette version.
Version en bleu signifie que c'est la 1ère version de la release

5.2 Contrôle des mots de passe et vérification des mots de passe

	Contrôle des mots de passe usager (système)	Management password control (system)	User, Management and Admin SIP Phone passwords check (system) AutoPwdChk	OMC user password check and reset (only with OMC910/14.1b and above)[2]
R3.1	*non dispo.*[1]	*non dispo.*[1]	*non dispo.*[1]	oui
R4.1	410/064.001	*non dispo.*[1]	*non dispo.*[1]	oui
R5.1	510/058.001	*non dispo.*[1]	*non dispo.*[1]	oui
R6.1	610/047.001	*non dispo.*[1]	*non dispo.*[1]	oui
R7.0	*non dispo.*[1]	*non dispo.*[1]	*non dispo.*[1]	oui
R7.1	710/057.007	*non dispo.*[1]	*non dispo.*[1]	oui
R8.0	800/030.002	*non dispo.*[1]	*non dispo.*[1]	oui
R8.1	810/045.003	*non dispo.*[1]	*non dispo.*[1]	oui
R8.2	820/026.007	*non dispo.*[1]	*non dispo.*[1]	oui
R9.0	900/033.002	*non dispo.*[1]	*non dispo.*[1]	oui
R9.1	910/021.001	910/021.001	910/021.001	oui
R9.2	toutes	toutes	toutes	oui
R10.0	toutes	toutes	toutes	oui

1: Non disponible signifie que cette fonction n'existe pas dans cette version.
2: la vérification et r-à-z des mots de passe usager par OMC fonctionnent sur toutes les versions.
Version en bleu signifie que c'est la 1ère version de la release

Suivez-nous sur Facebook et Twitter

Restez à l'écoute, sur nos réseaux Facebook et Twitter où nous vous informons de:

- Nouvelles publications de logiciels
- Nouvelles communications techniques
- Nouveaux rapports d'interopérabilité AAPP
- Lettre d'information
- Etc.


twitter.com/ALUE_Care


facebook.com/ALECustomerCare

Soumettre une demande de « Service Request»

Connectez-vous à l'application eService Request

Avant de soumettre une demande de «Service Request» assurez-vous:

- Que l'application a été certifiée via l'AAPP, au cas où une application tierce est impliquée.
- D'avoir pris connaissance des dernières mises à jour concernant les nouvelles fonctionnalités, les pré-requis systèmes, les restrictions, etc. disponibles dans la Technical Documentation Library
- D'avoir pris connaissance des Guides de dépannage et Bulletins Techniques associés à la demande, disponibles dans la Technical Documentation Library
- D'avoir consulté notre base d'articles tels que: les conseils techniques, comment faire, les problèmes connus, disponibles dans le Technical Knowledge Center

- FIN DU DOCUMENT -