

Kobium

Contenu

Logiciel Kobium.....	1
Introduction à l'entrée SSL.....	2
Caractéristiques.....	3
Objectif.....	3
Exemple de configuration 1 : Serveur Kobium autonome.....	4
Exemple de configuration 2 : Ferme Kobium avec 3 serveurs et 2 connexions internet.....	5
Maintenance.....	6
Etape 1 : Générer un Certificat de Serveur et une Bi-clé.....	6
Etape 2 : Permettre l'entrée SSL.....	8
Etape 3 : Générer un ou plusieurs Certificats de Client - et Bi-clés.....	9
Etape 4 : Générer une version du client.....	10
Installer la version d'installation du client.....	11
Vista : Contrôle d'accès de l'utilisateur (UAC).....	11
kobWin32client.exe.....	12
Détails de la version d'installation du client.....	13
Fonctionnement.....	15
L'entrée SSL et la ferme.....	15
Autres Certificats inconnus et Clés.....	16
Visualisation des Connexions SSL actives.....	17
Enregistrement des tentatives de connexions échouées.....	18
Journal des modifications.....	19
Contenu protégé par le copyright EXTREME TECHNOLOGIE.....	20
Parties protégées par d'autres copyrights.....	20

Introduction à l'entrée SSL

Caractéristiques

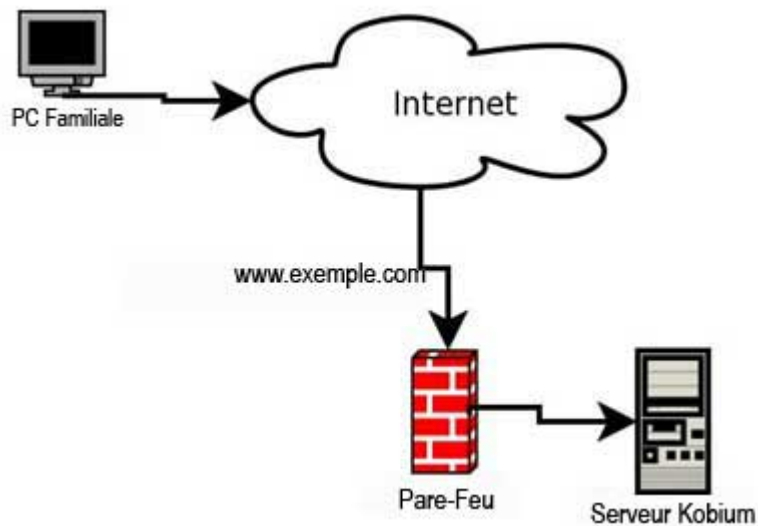
- Les certificats générés par l'Entrée SSL sont basés sur RSA, 2048 bits.
- Le client et le serveur vérifient tous deux leur certificat respectif.
- L'Entrée SSL peut être utilisée dans une Ferme Kobium.

Objectif

L'objectif de l'Entrée SSL est de fournir une session de bureau sécurisée entre n'importe quel endroit du monde et un serveur Kobium. Le terme "sécurisé" implique :

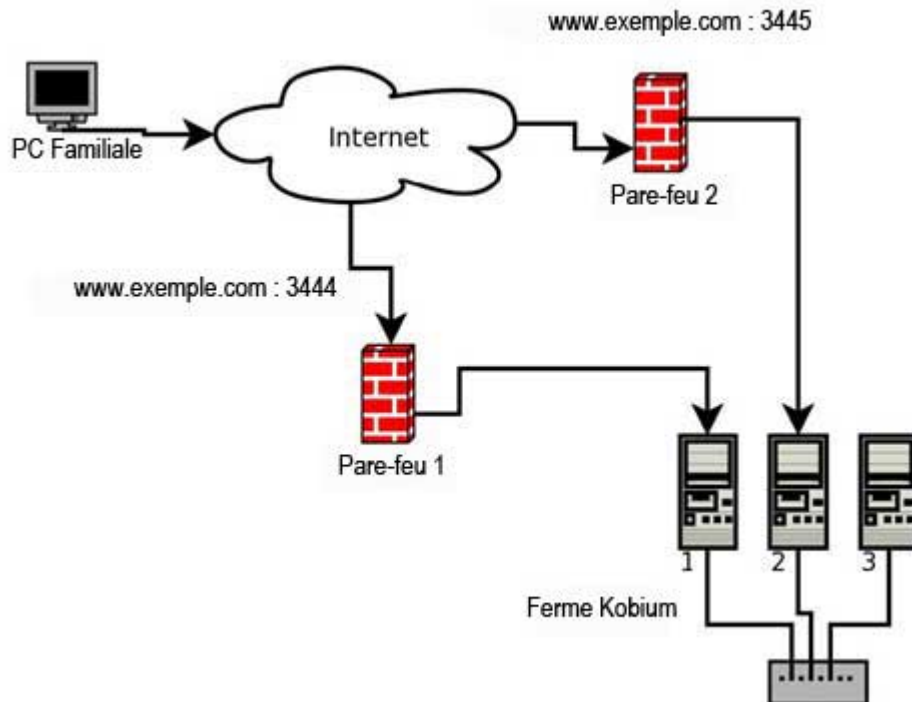
- Qu'un chiffrement SSL fort est utilisé afin d'éviter que la connexion ne soit « écoutée ». Le protocole RDP lui-même est déjà crypté, mais un chiffrement SSL associée à la connexion RDP, utilisant des certificats forts, sera plus efficace.
- Identification du client et du serveur. L'Entrée SSL donne la possibilité à un Administrateur de distribuer des versions spécifiques du Client, avec un certificat inclus, qui ne peuvent se connecter qu'à un ou plusieurs Serveurs Kobium. L'Administrateur peut également retirer un certificat de Client, de sorte que le client ne puisse plus se connecter.

Exemple de configuration 1 : Serveur Kobium autonome



- La compagnie a une connexion internet. Cette connexion est accessible par le nom de domaine `www.example.com`
- Le client qui utilise le PC principal se connecte via `www.example.com` : 3443.
- Le pare-feu redirige les connexions entrantes destinées au port 3443 vers le Serveur Kobium.
- Le Serveur Kobium exécute l'Entrée SSL sur le port 3443.
- Il s'agit d'un Serveur Kobium autonome ; il n'y a pas de Ferme Kobium.

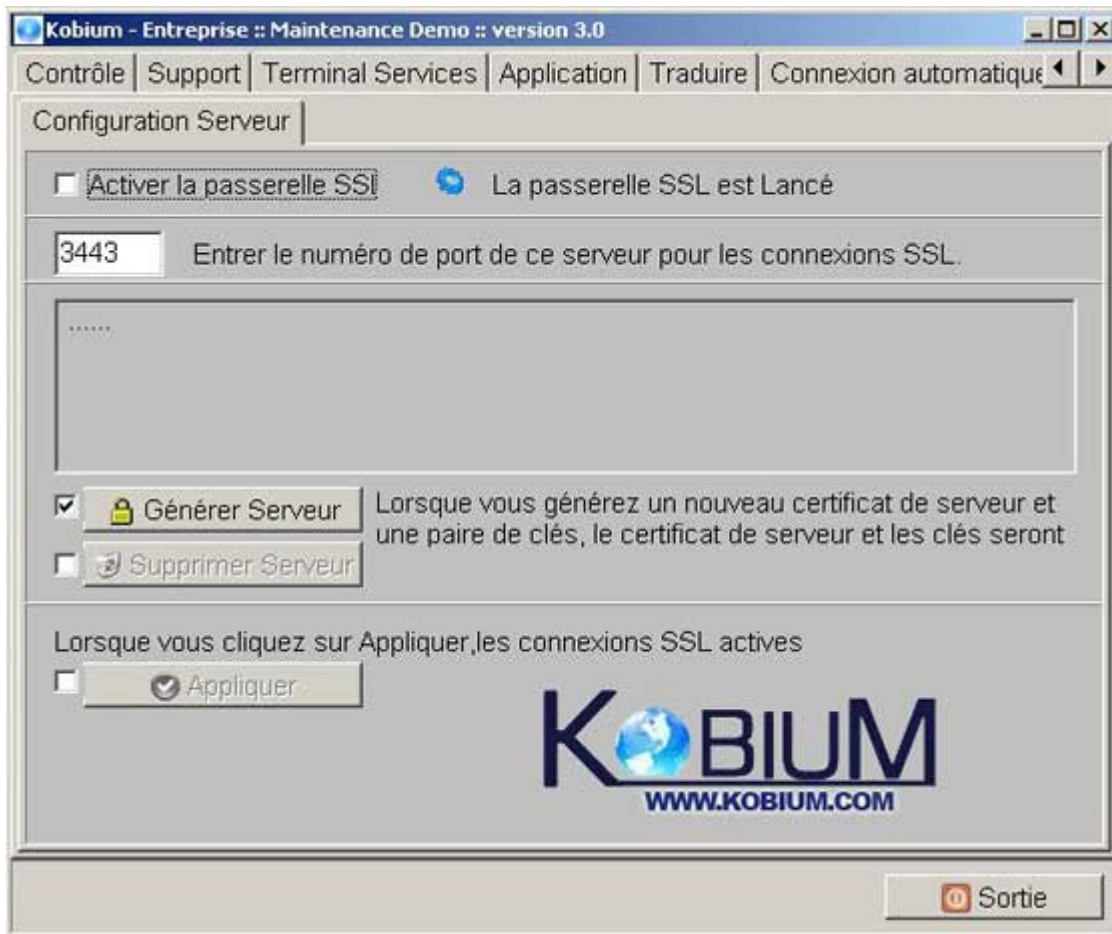
Exemple de configuration 2 : Ferme Kobium avec 3 serveurs et 2 connexions internet



- La compagnie possède deux connexions internet.
 - Quand un client essaie de se connecter à `www.exemple.com : 3444`, la connexion traverse le premier pare-feu.
 - Quand un client se connecte en utilisant `www.exemple.com : 3445`, la connexion traverse le second pare-feu.
- Le client du PC principal peut utiliser soit `www.exemple.com : 3444` soit `www.exemple.com : 3445`
 - En offrant deux adresses de connexion au client, et en ayant deux connexions internet, la compagnie peut offrir la redondance au client pour la connexion à la Ferme Kobium
- Le premier pare-feu redirige le port 3444 vers l'Entrée SSL sur le Serveur Kobium 1
- Le second pare-feu redirige le port 3445 vers l'Entrée SSL sur le Serveur Kobium 2
- Les Entrées SSL des Serveurs Kobium 1 et 2 assureront la redirection correcte vers le Serveur Kobium approprié au sein de la Ferme, à partir des paramètres d'équilibrage de charge.
- Le Serveur Kobium 3 n'exécute pas l'Entrée SSL

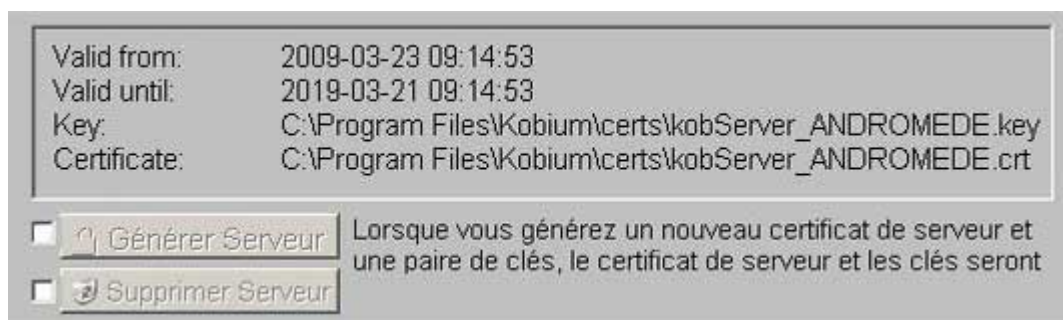
Maintenance

Etape 1 : Générer un Certificat de Serveur et une Bi-clé



Après une nouvelle installation de Kobium, le serveur n'a aucun certificat. Activez le bouton "Générer un Serveur", et vous pouvez générer un Certificat de Serveur et une Bi-clé.

- Le Certificat et la Bi-clé sont valables 10 ans
- Le Certificat contient le nom (netbios) du serveur



En utilisant le bouton Effacer du Serveur, vous pouvez effacer l'actuel Certificat de Serveur et la Bi-clé.

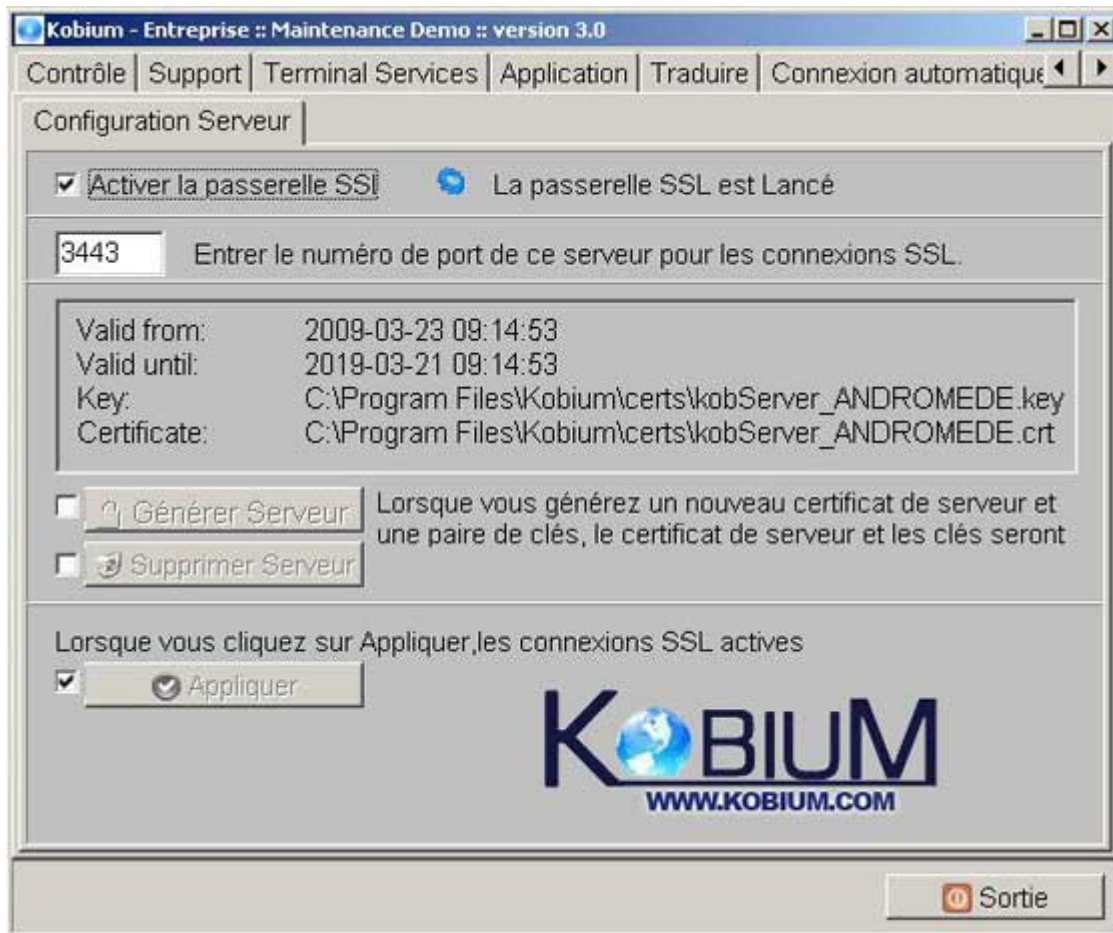
Important:

Le Certificat de Serveur (pas la Bi-clé) sera rendu disponible au Client. Si vous effacez l'actuel Certificat de Serveur - et la Bi-clé, et que vous générez une nouvelle Bi-clé, vous devrez distribuer une version d'installation du Client à tous vos clients afin de leur fournir le nouveau Certificat de Serveur.

Après avoir effacé l'actuel Certificat de Serveur - et la Bi-clé, il n'est plus possible pour aucun Client qui possède l'actuel Certificat de Serveur, d'établir une connexion avec le Serveur.

Par conséquent, soyez prudent avec l'effacement de l'actuel Certificat de Serveur - et de la Bi-clé. Utilisez-le uniquement de manière délibérée, lorsque vous ne voulez pas que les Clients qui connaissent l'actuel Certificat de Serveur soient capables d'établir une connexion avec le Serveur.

Etape 2 : Activer l'entrée SSL



Activez l'Entrée SSL en utilisant la case à cocher du haut et cliquez sur le bouton Appliquer. Le statut "Activé ou désactivé " de l'Entrée SSL apparaîtra.

L'activation de l'Entrée SSL active également les onglets suivants.

Etape 3 : Générer un ou plusieurs Certificats de Client - et des Bi-clés

Nom du client	Numéro de serie	V
ANDROMEDE_exemple	ED9F2258034212D7F73D92	
ANDROMEDE_exemple2	077C4DEF4D9DA9817AD32	
ANDROMEDE_exemple3	2F70F16FA43DD2D50692F2	

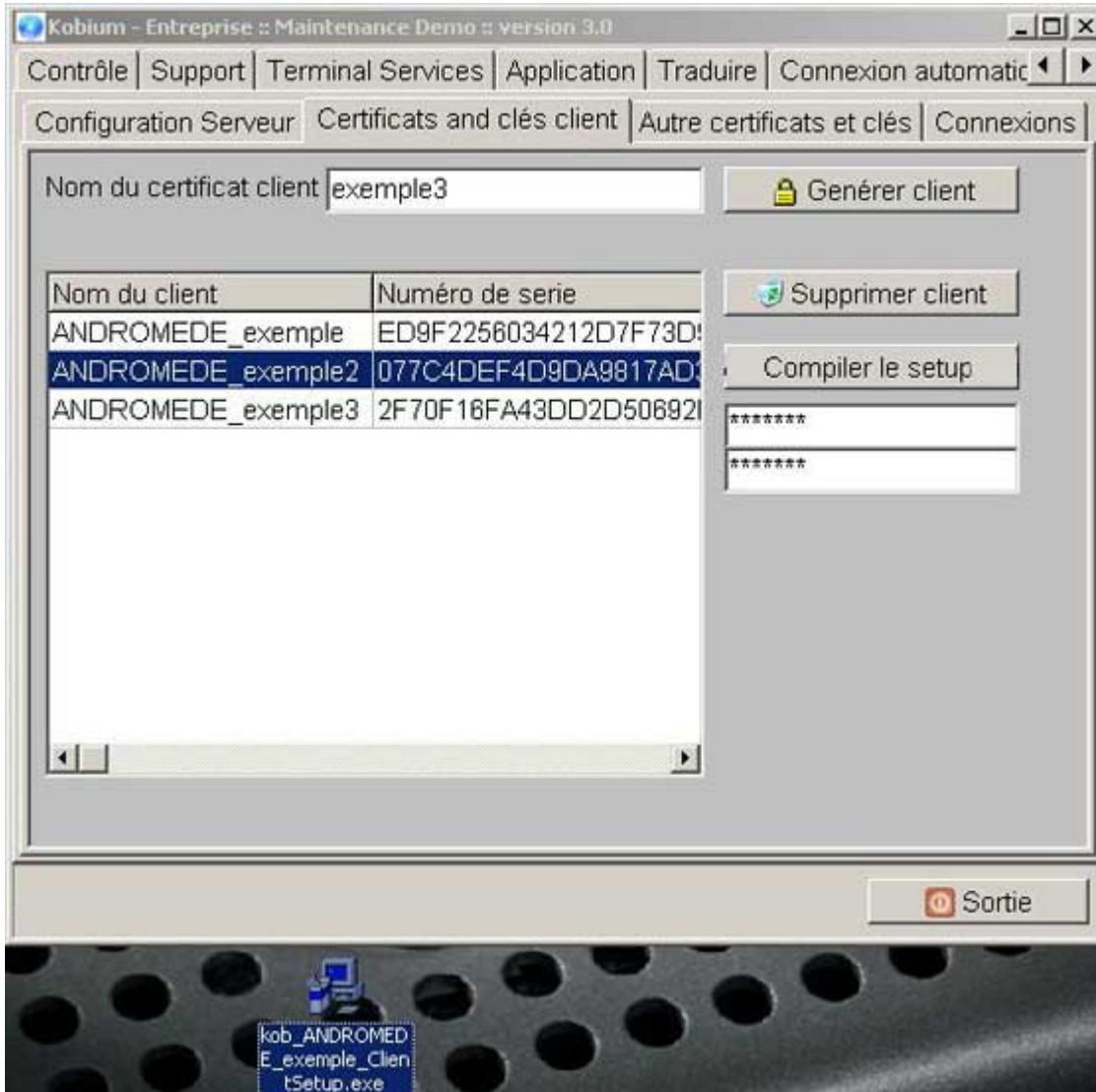
Entrez un nom pour le client.

- Le nom est au moins 4 places.

Vous pouvez générer un Certificat séparé - et une bi-Clé - pour chaque individu. Vous pouvez également choisir de générer un Certificat d'"utilisateur fonctionnel" - et une Bi-clé, par exemple une Bi-clé pour les employés du service Vente.

En utilisant le bouton « Effacer » du Client, le Certificat ainsi que la Bi-clé de l'utilisateur sélectionné seront effacés. Les utilisateurs possédant ce Certificat - et cette Bi-clé, ne seront plus capables d'établir une connexion avec le Serveur.

Etape 4 : Générer une version de client



- Sélectionnez un Certificat de Client - et une Bi-clé.
- Entrez un mot de passe (facultatif). L'utilisateur à qui la version d'installation du Client est destinée, devra entrer ce mot de passe lorsqu'il installera la version d'installation du Client.
- Cliquez sur le bouton « Version d'installation du Client ».

Sur le bureau de l'Administrateur sera créé un fichier EXE contenant la version d'installation complète du Client pour l'utilisateur sélectionné.

- Attribuez la version d'installation du Client à l'utilisateur concerné.

Installer la version d'installation du client

- Attribuez la version d'installation du Client -Exe à l'utilisateur concerné.

La seule chose que l'utilisateur ait à faire est de double-cliquer sur le fichier Exécutable.

- La version d'installation du Client -Exe exige des droits d'Administrateur sur le PC Client afin d'être installée.

Une installation s'achève avec succès lorsque le message suivant apparaît :



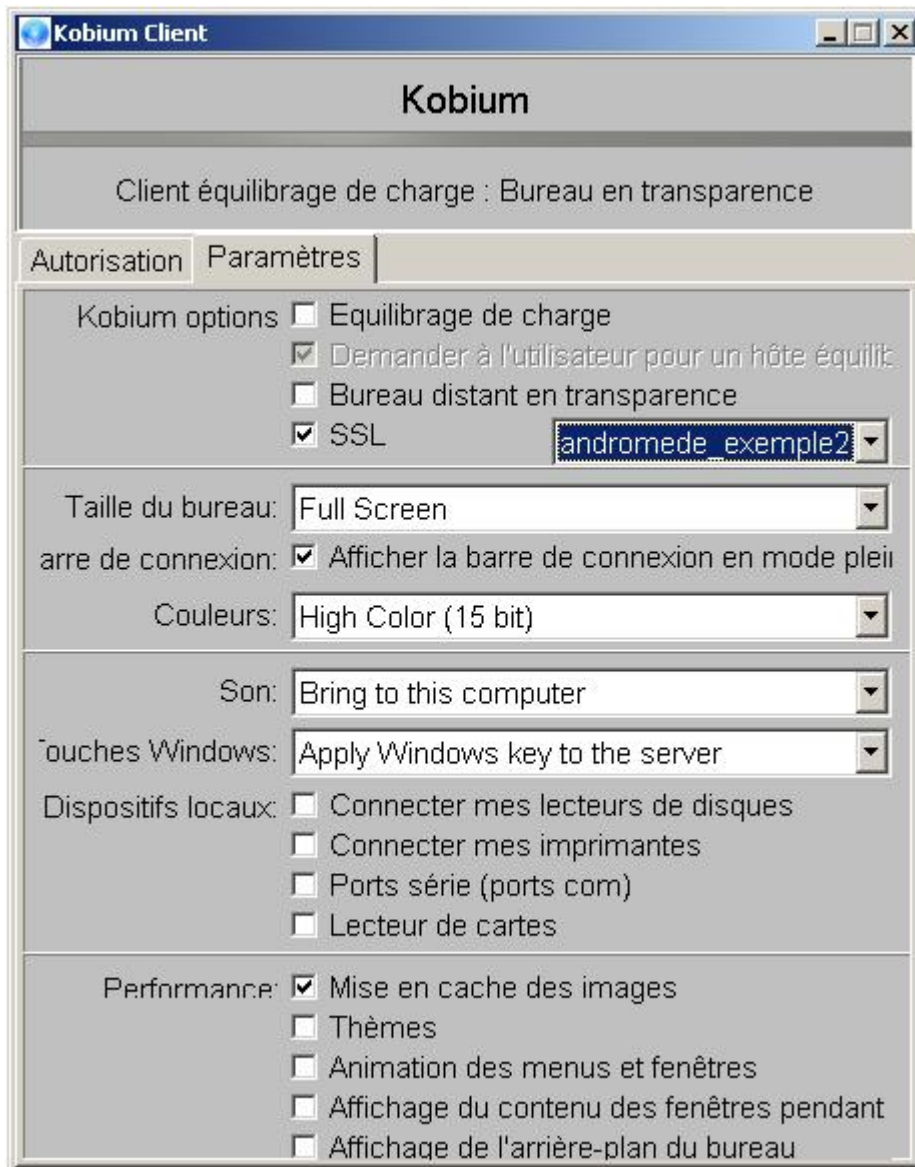
- Une entrée est placée dans le Menu Démarrer du PC
- La version d'installation du Client peut être désinstallée du PC en utilisant Ajouter / Supprimer un programme

Vista : Contrôle d'accès de l'utilisateur (UAC)

Les certificats sont installés de telle sorte que chaque utilisateur d'un PC Vista peut « lire » les certificats. Les utilisateurs ne peuvent pas ajouter ou supprimer des certificats.

Kobium.exe

Le programme du client kobiumWin32client possède une option supplémentaire pour la connexion SSL :



Cochez la case « Utiliser SSL » et sélectionnez le Certificat. Généralement, une version d'installation du Client ne contient qu'un seul Certificat et une seule Bi-clé ; il n'y a donc pas beaucoup de choix...

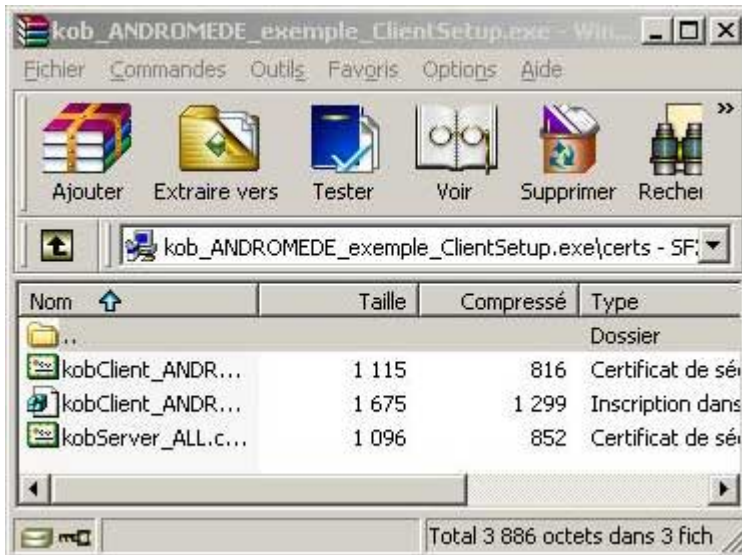
Détails de la version d'installation du client

Les détails de la version d'installation du Client apparaissent lorsque vous l'ouvrez avec WinRAR, par exemple :



- Lorsque l'utilisateur double-clique sur la version d'installation du Client, cette dernière exécute le programme ClientSetup.exe.
- La langue incluse est la même que celle qui est installée sur le serveur Kobium.
- L' * derrière les noms de dossier indique qu'il y a une protection du mot de passe sur chaque dossier. C'est le mot de passe que l'Administrateur a entré lors de l'étape antérieure.

Le dossier Certs contient les Certificats - et les Clés :



- Il contient uniquement le Certificat - et la Bi-clé de l'utilisateur concerné.
- Le fichier kobServer_All.crt contient tous les Certificats de Serveur. Dans le cas d'une Ferme Kobium, il y aura un Certificat de Serveur pour chaque Serveur de la Ferme.

Important :

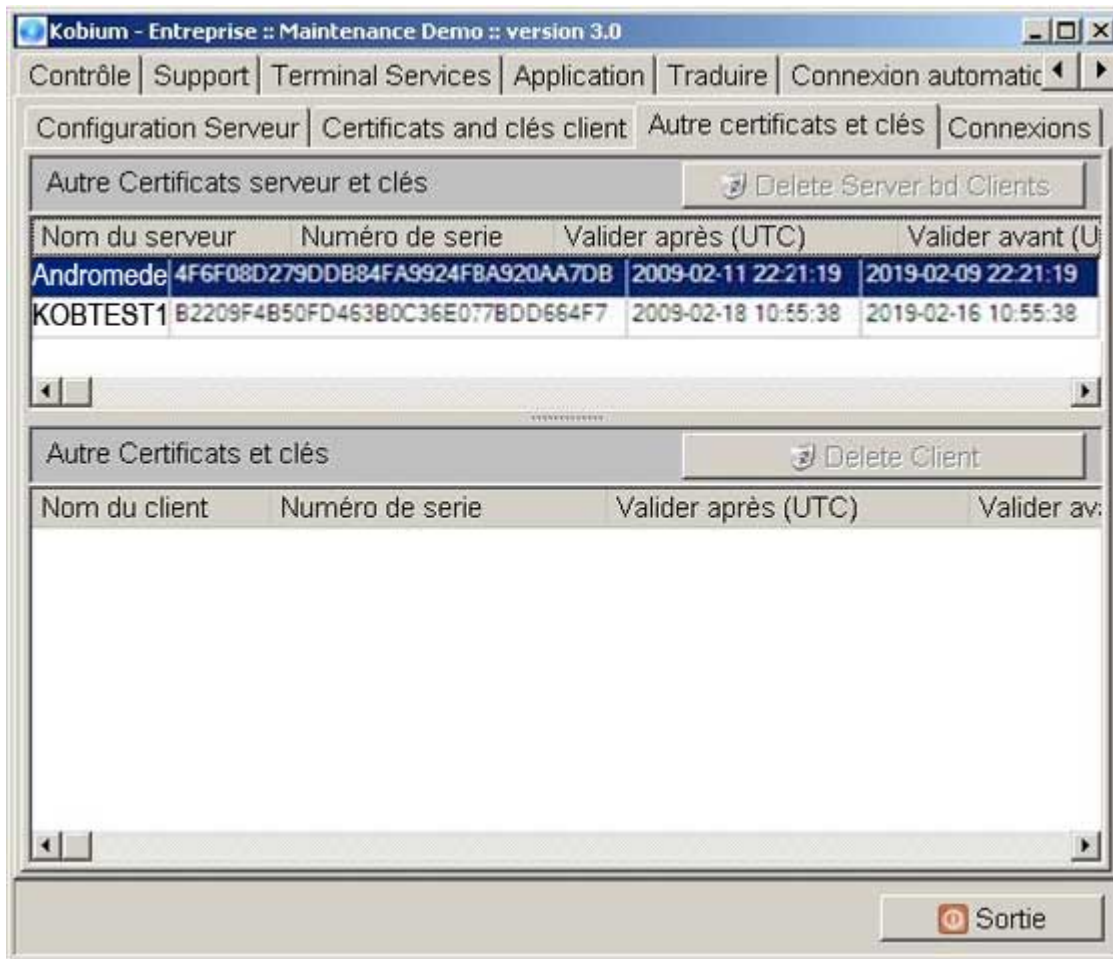
L'utilisateur doit savoir qu'il / elle doit être prudent avec le dossier clé *. Si ce dossier clé tombe entre les mains d'autres personnes, quelqu'un d'autre peut se faire passer pour l'utilisateur en effectuant une connexion SSL.

Si cela se produit, l'Administrateur doit effacer le Certificat de Client - et la Bi-clé, comme expliqué dans l'étape 3, en utilisant le bouton « Effacer le Client ».

Fonctionnement

L' Entrée SSL et la ferme

Si le Serveur fait partie d'une Ferme Kobium, les Serveurs de la Ferme s'informeront les uns les autres à propos des Certificats :



Autres Certificats et Clés inconnus

Si un serveur dans la Ferme est en panne, ou si un serveur est supprimé de manière permanente, les autres serveurs ne « reconnaissent » plus les Certificats et les Clés. Voici ce qui apparaît alors :

Nom du serveur	Numéro de serie	Valider après (UTC)	Valider avant (UTC)
AMD64	6810C884C0FCD7A0608CDC84630410A8	2009-02-25 16:30:50	2019-02-23 16:30:50
RBR-PC	B381102041CA7F889AD108B3E58318CF	2009-02-22 19:31:15	2019-02-20 19:31:15
WIN-H3C1E66V8FI	5435950658EABD31A11AA3407318EF85	2009-02-27 18:24:33	2019-02-25 18:24:33
KOBTEST1	B2209F4B50FD46380C36E0778DD664F7	2009-02-18 10:55:38	2019-02-16 10:55:38
KOBTEST2	C065C557A0169CEA8C86344A88545A3F	2009-03-01 19:42:58	2019-02-27 19:42:58

Nom du client	Numéro de serie	Valider après (UTC)	Valider avant (UTC)
WIN-H3C1E66V8FI	EA9623D095E84CAF7478AD6F166426D0	2009-03-01 19:20:47	2019-02-27 19:20:47
WIN-H3C1E66V8FI	C6454EA5483EBEB1BCD907A268E7E32C	2009-03-01 19:20:55	2019-02-27 19:20:55
KOBTEST1_exemple	E3882FD1909DE85266D7C840FE68497C	2009-02-18 10:55:57	2019-02-16 10:55:57
KOBTEST2_exemple2	0912BEDDFE48DBE1A93E2C273219730E	2009-03-01 19:43:43	2019-02-27 19:43:43
KOBTEST2_exemple3	EF42EA94F111922D5D011719447C8177	2009-03-01 19:43:20	2019-02-27 19:43:20

- Les Serveurs AMD64, RBR-PC et KOBTEST2 ne sont pas disponibles dans la Ferme. Ces serveurs sont autonomes et hors ligne.
- L'Administrateur a généré deux Certificats de Client sur le Serveur KOBTEST2, appelés charlie et williams. Les deux Certificats de Client sont distribués au sein de la Ferme.

L'Administrateur peut effacer ces Certificats inconnus en utilisant les boutons Effacer.

Veillez noter que lorsque vous effacez par hasard les Certificats et les Clés d'un serveur qui est seulement en panne temporairement, ce n'est pas un gros problème. Lorsque ce serveur

temporairement en panne est de retour dans la Ferme, il distribuera automatiquement ses Certificats et ses Clés au sein de la Ferme.

Visualisation des connexions SSL actives

Les connexions actives peuvent être visualisées dans l'onglet suivant :

Certificat	Client	Serveur	Utilisateur	Temps de connexion
ANDROMEDE_exemple 4395f6040e6ccec5e0cedae951497183	DEVELOP 192.168.200.130	KOBTEST1 192.168.200.241	/ domain003	28-01-2009 09:23:22 00:01:37
ANDROMEDE_exemple2 514e312edfa951438363dc46632fd96	CLIENT1 192.168.200.231	KOBTEST2 192.168.200.242	TESTXP.INTERN/ domain001	28-01-2009 09:24:36 00:00:23
ANDROMEDE_exemple2 514e312edfa951438363dc46632fd96	CLIENT2 192.168.200.232	ANDROMEDE 192.168.200.162	TESTXP.INTERN/ domain002	28-01-2009 09:24:48 00:00:11

- L'exemple montre deux PC différents qui utilisent tous deux le même Certificat de Client SSL. Apparemment, la version d'installation du Client qui contient le certificat JEWEL_rene est installée sur deux PC.
- Le Serveur Kobium, dans l'exemple ci-dessus, fait partie d'une Ferme Kobium. Basé sur les paramètres d'équilibrage de charge, l'Entrée SSL a redirigé chaque session vers le serveur approprié de la Ferme Kobium.
- Les noms tels que DEVELOP, CLIENT1, KOBTEST1, etc, dans l'exemple ci-dessus, sont les noms (netbios) de PC ou de Serveur.

Erreurs lors de l'authentification

Dans le dossier \windows\temp, vous trouverez un fichier d'authentification qui est créé à chaque fois qu'une connexion SSL échoue. Par exemple, si un Certificat de Client et une Bi-clé sont

supprimés et qu'un utilisateur continue d'essayer de se connecter au serveur Kobium en utilisant ce Certificat de Client et cette Bi-clé pour s'authentifier, cela fonctionnera.

Journal des modifications

4 mars 2009	Mise à jour du manuel <ul style="list-style-type: none"> • Information concernant les certificats et le Contrôle d'Accès de l'Utilisateur (UAC)
1 mars 2009	Introduction d'un bouton pour effacer les certificats et les clés "inconnus"
4 février 2009	Suppression d'un bug <ul style="list-style-type: none"> • Une panne du serveur Kobium pouvait se produire sur les processeurs multi-cœurs
27 janvier 2009	Première sortie de l'Entrée SSL

Tout le contenu est sous le copyright d' Extreme Technologie

Extreme Technologie

Mail : info@extreme-technologie.com

Web : <http://www.extreme-technologie.com>

Parties protégées par d' autres copyright

L'Entrée SSL est fondée sur et inspirée des composants TCP/IP d'Indy. Visitez www.indyproject.org pour plus d'informations.

L'Entrée SSL utilise des bibliothèques OpenSSL. Visitez www.openssl.org pour plus d'informations.