

# Installation Corporate Desk

CORPORATE COPYRIGHT	Version : 2.0
Nom du fichier : Installation Corporate Desk.doc	Date de création : 28/03/2015 11:56:00 Dernière sauvegarde : 23/06/2017 16:17:00
Type de document :	Description fonctionnelle
Historique du document :	
2.0	• Répertoire local

1	Installation.....	2
1.1	Droits requis .....	2
2	Vérification de l'installation .....	2
3	Mise à jour de l'installation .....	3
3.1	Méthode automatique.....	3
3.2	Méthode manuelle.....	4
3.3	Importation.....	4
3.4	Répertoire local .....	5
3.4.1	Fournisseurs du répertoire local .....	5
3.4.2	Clients du répertoire local .....	5
3.5	Outil externe.....	5
4	Historique des mises à jour .....	6
5	Installation corrompue .....	6
6	Antivirus.....	7
7	Outils disponibles.....	8

# **1 Installation**

L'installation peut être faite avec le setup le plus récent, disponible en le téléchargeant depuis [www.corporate.be/corporatedesk/FR/setup.zip](http://www.corporate.be/corporatedesk/FR/setup.zip).

Le logiciel est conçu pour être installé localement (hormis Terminal Server), il n'est pas prévu pour être installé sur un serveur de fichiers à partir duquel plusieurs utilisateurs pourraient exécuter chacun une instance de la même installation. Outre le fait que les performances pourraient être dégradées (l'application est modulaire et charge et décharge très régulièrement des bibliothèques : tout cela se ferait à travers le réseau), le problème le plus important est le risque de corruption de l'installation, ce qui pourrait arriver si par exemple un des utilisateurs tente une mise à jour alors que d'autres utilisateurs sont en cours de travail.

Vous pouvez évidemment installer le logiciel où vous le souhaitez, mais le plus simple est de suivre les standards Windows et de l'installer dans le répertoire « C:\Program Files » (ou « C:\Program Files (x86) » sur les ordinateurs 64 bits), tel qu'il est proposé par le setup.

## ***1.1 Droits requis***

Quel que soit le répertoire d'installation, l'utilisateur Windows qui fait l'installation doit avoir les droits d'administrateur, et de préférence faire partie du groupe administrateur. En effet, non seulement le setup doit avoir les droits d'écriture sur le répertoire d'installation, mais il doit aussi avoir les droits d'administrateur sur la Registry de Windows, afin de pouvoir enregistrer l'application. A défaut, l'enregistrement aura lieu dans une section spéciale de la Registry (virtualisation), section qui sera invisible par d'autres utilisateurs Windows : dans ces conditions, un utilisateur standard Windows (ou tout autres utilisateur Windows d'ailleurs) ne verra pas cette configuration et sera incapable de démarrer l'application.

Plus exactement, l'utilisateur doit avoir les droits sur les éléments suivants :

- Des droits d'écriture sur le répertoire où l'application est installée (par défaut : « C:\Program Files\Corporate\CorporateDesk » ou « C:\Program Files (x86)\Corporate\CorporateDesk » sur un ordinateur 64 bits). Au minimum le droit d'y copier ou d'y remplacer des fichiers, mais si possible aussi le droit d'y supprimer des fichiers
- Des droits d'écriture sur la clé « HKEY\_LOCAL\_MACHINE\Software\Corporate\CorporateDeskAppl » de la registry (« HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Corporate\CorporateDeskAppl » sur une machine 64 bits)

## **2 Vérification de l'installation**

Avec l'installation, est fourni un module qui est en fait une véritable carte d'identité de l'installation. C'est avec ce module « carte d'identité » que l'application peut dire quelle version elle présente, mais également si elle est intègre et complète. Une installation peut s'avérer corrompue par rapport à cette « carte d'identité » si par exemple (liste non exhaustive) :

- La dernière mise à jour est incomplète, pour quelque raison que ce soit
- Un module de l'installation a été effacé par accident
- Un module a été mis en quarantaine par l'antivirus (que ce soit valablement ou indûment)

Si cette situation est détectée, l'installation doit être réparée, voir plus loin.

Cette vérification intervient à chaque démarrage de l'application : ceci permet d'être sûr (ou à peu près) que l'application que l'on démarre est intègre ou non. Il est sans doute préférable de voir le démarrage de l'application interrompu par un message de corruption, que de travailler avec celle-ci, peut-être durant des heures, et puis de voir son travail perdu parce que la dernière opération que l'on souhaite exécuter échoue parce que le module correspondant est corrompu.

Vous pouvez également vérifier l'installation vous-même :

- Dans l'application : menu « Aide », « A propos de », bouton « Détails »
- Dans le panneau de configuration, option « Configuration détaillée de l'application »

Dans les 2 cas, vous obtenez la liste des modules, avec pour chacun la version attendue et la version trouvée. Si l'installation est correcte, la mention « Installation correcte » apparaît dans le haut de l'écran. Sinon, apparaît une sélection « Tous les modules » et « Modules incorrects » : sélectionner ce dernier point limite l'affichage aux modules dont l'installation trouvée n'est pas conforme à l'installation attendue

### **3 Mise à jour de l'installation**

Il y a diverses méthodes de mise à jour de l'installation :

1. Méthode automatique
2. Méthode manuelle
3. Importation d'une mise à jour
4. Répertoire local
5. Outil externe

Il est à noter que le setup est aussi une méthode de mise à jour, mais ce dernier ne contient pas toujours la toute dernière release. En effet, le concept des mises à jour a été conçu pour permettre des mises à jour très rapides, et ainsi pouvoir être très réactif soit à une modification des contraintes du SPF, soit à la correction d'un bug empêchant l'utilisation normale du logiciel. Il peut donc arriver qu'une mise à jour soit mise à disposition, sans pour autant que le dernier setup n'intègre cette modification.

Le dernier setup est toujours disponible depuis [www.corporate.be/corporatedesk/FR/setup.zip](http://www.corporate.be/corporatedesk/FR/setup.zip)

Par ailleurs, la mise à jour, quelle que soit la méthode, requière également que l'utilisateur Windows qui l'exécute soit dans le groupe administrateur, pour les mêmes raisons que lors de l'installation.

#### ***3.1 Méthode automatique***

La plus simple est la méthode automatique. Au démarrage, l'application se met en connexion avec le serveur de mises à jour et compare l'installation locale avec celle proposée sur le serveur. Si elles sont identiques (ce qui est le cas dans la majorité des cas), le démarrage continue sans rien dire : l'application est à jour. Mais s'il y a discordance, si l'installation locale est plus ancienne que celle proposée sur le serveur de mises à jour, la mise à jour de l'installation locale est proposée ou au moins annoncée, selon les droits de l'utilisateur qui exécute l'application. Vous pouvez remettre

cette mise à jour à plus tard (ce peut être le cas par exemple si l'utilisateur voit que la mise à jour concerne le module « Fiches 281 » alors qu'il est occupé à introduire les déclarations TVA), ou vous pouvez l'accepter (ce qui est conseillé dans la majorité des cas). Dans ce cas, la mise à jour est téléchargée, puis l'instance courante de l'application est arrêtée, l'application est mise à jour et ensuite elle est redémarrée. En cas d'échec de la mise à jour, l'application fait dans la mesure du possible un « rollback », c'est-à-dire qu'elle revient pour autant que possible à la situation qui prévalait avant la tentative de mise à jour.

A noter que pour que la mise à jour puisse être effectuée, il faudra que l'utilisateur ait les droits d'administrateur, et plus exactement qu'il soit membre du groupe administrateur. Cela signifie qu'au moment de la mise à jour proprement dite, l'application requerra éventuellement une élévation des droits de l'UAC.

Par défaut, cette vérification n'a lieu qu'une fois par jour. Cela signifie que si vous démarrez l'application plusieurs fois le même jour, elle va vérifier sa situation la première fois, mais ne fera plus cette vérification les fois suivantes.

Vous pouvez ajuster ce comportement dans le menu « Fichier », « Préférences », onglet « Internet » : là, vous sélectionnez soit « A chaque démarrage », soit « 1 fois par jour », soit « tous les ... jours » et vous précisez le nombre de jours (entre 2 et 30). Attention, il faut que la case « travailler hors connexion » soit décochée.

### **3.2 Méthode manuelle**

Vous pouvez également faire une mise à jour manuelle. Le mécanisme est sensiblement le même, sauf qu'il n'est pas exécuté automatiquement au démarrage, vous le provoquez vous-même. Ce peut être utile par exemple si la mise à jour automatique au démarrage a échoué, ou encore si a priori vous travaillez off-line.

Pour faire cette mise à jour manuelle, vous allez dans le menu « Fichier », « Préférences », onglet « Internet » et vous cliquez sur « Mise à jour manuelle ». Vous pouvez aussi aller dans le panneau de configuration de l'application, option « Configuration détaillée de l'application », bouton « Mise à jour ». A part le fait que vous provoquiez cette mise à jour de manière volontaire (par le click sur un bouton), le fonctionnement est identique à la mise à jour automatique. Et en particulier, une élévation éventuelle des droits de l'utilisateur peut être requise. Que ce soit via l'application ou via le panneau de configuration, la mise à jour ne sera effective qu'après arrêt de l'application en cours, mais il n'y aura pas de redémarrage automatique.

*Exemple : vous faites la mise à jour manuelle dans l'onglet « Internet » des préférences dans Corporate Desk. La mise à jour est téléchargée et mise en attente. Vous continuez à travailler avec l'ancienne version, la nouvelle version ne sera installée que lors de la fermeture de Corporate Desk, et ne sera donc disponible que lors du prochain démarrage.*

### **3.3 Importation**

Vous pouvez également télécharger une mise à jour et l'importer dans l'application. L'avantage de cette méthode est que la mise à jour peut être téléchargée sur un poste distinct de celui où l'application est exécutée, par exemple parce que ce poste n'est pas connecté à Internet ou parce que le proxy ou le firewall l'empêche. La mise à jour de l'application peut être importée depuis [www.corporate.be/corporatedesk/patch <version produit>.upd](http://www.corporate.be/corporatedesk/patch<version produit>.upd), où la version du produit doit être

indiquée en minuscules. Par exemple, avec la version X.15a, la mise à jour peut être téléchargée depuis [www.corporate.be/corporatedesk/patch\\_x.15a.upd](http://www.corporate.be/corporatedesk/patch_x.15a.upd).

Ensuite vous allez dans le menu « Fichier », « Préférences », onglet « Internet », bouton « Importation mise à jour », vous sélectionnez le fichier téléchargé et vous suivez les instructions. Notez que encore une fois, une élévation des droits de l'utilisateur peut être requise. Comme pour une mise à jour en ligne, la mise à jour ne sera effective qu'après redémarrage de l'application.

Cette importation peut également être faite dans le panneau de configuration : « Configuration détaillée de l'application », bouton « Importation mise à jour ».

### **3.4 Répertoire local**

Les procédures ci-dessus sont valables individuellement pour chaque poste. Mais dans un réseau, il est possible que certains postes soient connectés à Internet, tandis que d'autres ne le sont pas. Ou que les accès à Internet à travers un proxy soient différents d'un poste à l'autre.

Il est dès lors possible pour un poste du réseau ayant accès à Internet, de télécharger la mise à jour, de l'installer pour son propre compte, mais aussi de la partager avec les autres postes via un répertoire local accessible à tous les postes concernés.

#### **3.4.1 Fournisseurs du répertoire local**

Les fournisseurs du répertoire local sont ceux qui ont accès à Internet. Ils configurent leur poste comme indiqué ci-dessus dans la rubrique « Automatique », mais en plus ils sélectionnent (avec le bouton « ... ») un répertoire local dans le champ « Copie dans ».

Ce répertoire est quelconque, mais il doit bien entendu être accessible à tous les postes du réseau, par exemple sur un serveur de fichiers. Il est conseillé d'utiliser un répertoire uniquement pour cet usage, mais ce n'est pas obligatoire. L'application va créer dans ce répertoire un sous-répertoire en rapport avec la version en cours (« X.15a » par exemple).

Le répertoire local est alimenté également lors d'une mise à jour manuelle ou encore lors de l'importation d'une mise à jour. Pour annuler cette fonctionnalité, il suffit de vider le champ « Copie dans ».

#### **3.4.2 Clients du répertoire local**

Les clients du répertoire local sont ceux qui vont mettre leur version de Corporate Desk à jour en lisant les mises à jour dans ce répertoire local. Ils n'ont pas besoin d'avoir accès à Internet, mais ils doivent bien entendu avoir les droits requis pour faire la mise à jour (droits d'administrateur, comme expliqué plus haut).

Pour activer cette fonctionnalité, dans l'onglet « Internet » des préférences, il suffit de cocher « Extraire les mises à jour depuis », et de sélectionner le répertoire local approvisionné par les « fournisseurs ».

### **3.5 Outil externe**

Une dernière possibilité consiste à utiliser l'outil « CheckCDUpdate.exe ». Cet outil a été conçu essentiellement pour le monde « Terminal Server », mais il n'est pas limité à ce monde. Il est utile

en particulier si l'utilisateur habituel de l'application n'a pas les droits requis pour faire une mise à jour : dès qu'une mise à jour est disponible, l'administrateur système peut exécuter cet outil sans devoir démarrer l'application.

Une autre utilisation potentielle est de faire tourner cet outil automatiquement toutes les nuits (par exemple), et en contrepartie de ne plus vérifier les mises à jour lors du démarrage de l'application (voir menu « Fichier », « Préférences », onglet « Internet »)

Cet outil est autonome : il peut être déplacé et recopié n'importe où, et exécuté depuis cet emplacement distinct. Mais il faut bien entendu que ce soit sur l'ordinateur où l'application est installée.

Le fonctionnement détaillé de cet outil est décrit dans un autre document associé au Terminal Server.

## **4 Historique des mises à jour**

A tout moment, l'utilisateur peut connaître l'historique des mises à jour. Cette possibilité est proposée dans le menu « Aide » de l'application, mais aussi lors de l'affichage de la configuration de l'installation (liste des modules).

Il est important de noter que ce n'est pas l'historique des mises à jour installées, mais bien l'historique des mises à jour proposées. Si l'installation locale n'est pas à jour, cet historique permettra de voir quelles sont les mises à jour qui manquent, et ce qu'elles contiennent.

## **5 Installation corrompue**

Comme indiqué plus haut, lorsque l'application est démarrée, son intégrité est vérifiée. Cette vérification est faite également dans l'option « configuration détaillée de l'application » dans le panneau de configuration de l'application, ainsi que dans l'outil « CheckCDUpdate », ce qui donne 3 canaux possibles de réparation. A noter que l'outil « CheckCDUpdate » étant autonome, il peut toujours être utilisé, sauf si bien sûr il est lui-même défaillant.

Si l'installation est correcte, ce qui est normalement le cas, cette vérification est transparente.

Si elle n'est pas correcte, plusieurs cas peuvent se présenter :

- L'absence ou l'obsolescence d'un module optionnel est détectée : vous en êtes averti, mais vous pouvez continuer à travailler  
*Exemple : un module d'impression manque ou est désuet : vous pouvez introduire vos déclarations et les exporter, mais si vous tentez de les imprimer, soit vous ne pourrez pas, soit vous ne bénéficierez pas des derniers amendements*
- L'absence ou l'obsolescence d'un module indispensable est détectée : vous en êtes averti, et vous êtes invité à réparer. L'application retrouve alors le ou les modules manquants sur Internet et tente autant que possible la réparation de l'installation
- L'absence ou l'obsolescence d'un module critique est détectée : c'est le cas notamment si un des modules capables d'effectuer la réparation est concerné. Dans ce cas, vous en êtes averti, et vous devez utiliser un autre des canaux possibles de réparation.  
*Exemple : Corporate Desk détecte que le module « WebAccess.dll » est défaillant ; ce module est chargé des connexions avec le serveur, et sa défaillance empêche donc la*

*réparation immédiate. La solution alors est d'utiliser l'outil « CheckCDUpdate.exe », qui est autonome. La réparation avec le panneau de configuration n'est pas une solution car il utilise le même module.*

- Enfin, la corruption de l'installation peut être telle que l'application ne démarre plus .  
*Exemple : le module « CorporateDesk.exe » a disparu. Dans ce cas, l'application ne peut plus être démarrée, évidemment. La solution est d'utiliser un des autres canaux possible : le panneau de configuration ou l'outil « CheckDBUpdate »*

Ce processus peut également générer un rapport de réparation que vous pouvez exporter et renvoyer à Corporate Copyright pour analyse.

Tout ce processus suppose que l'ordinateur est on-line et a accès au serveur de mises à jour. Si ce n'est pas le cas, seul le rapport de réparation sera disponible, mais la réparation ne pourra évidemment pas être effectuée. Le plus simple est alors d'utiliser le dernier setup pour faire la réparation (éventuellement en le téléchargeant sur un autre ordinateur, connecté à Internet).

Mais vous pouvez également utiliser ce rapport de réparation pour télécharger sur un autre ordinateur un patch de réparation contenant les modules à réparer, copier ce patch sur l'ordinateur posant problème et l'importer, soit directement dans l'application (si la défaillance n'est pas trop importante), soit dans le panneau de configuration. La procédure est alors la suivante :

- Lorsque le besoin de réparation est annoncé, vous cochez la case « exporter et envoyer un rapport de configuration » et vous fermez. Le rapport ne sera évidemment pas envoyé si vous êtes off-line, mais il sera disponible dans votre répertoire « Mes Documents » sous le nom « CorruptionFileReport.txt »
- Vous copiez ce rapport sur un ordinateur connecté à Internet, ainsi que l'outil « DownloadRepairTool.exe »
- Vous exécutez l'outil « DownloadRepairTool », vous sélectionnez le rapport de configuration et un patch de réparation sera téléchargé
- Vous recopiez ce patch de réparation sur l'ordinateur où se trouve l'application et vous l'importez dans le panneau de configuration (ou dans l'application si c'est possible)

Si aucune de ces solutions ne fonctionne, il ne reste que le dernier setup.

## **6 Antivirus**

Le cas des antivirus est un cas particulier. Il se peut qu'un antivirus mette en quarantaine (ou même supprime) un module parce qu'il le considère comme infecté. Cette détection peut être réelle (le module est réellement infecté), ou induite (« faux positif ») : il peut arriver que dans le cadre d'une recherche heuristique, l'antivirus détecte un bout de code qu'il considère comme suspect alors qu'il n'en est rien.

Si le module écarté par l'antivirus est réellement infecté, la procédure de réparation (quelle qu'elle soit) va installer une nouvelle version du module écarté, non infectée, et la réparation sera normalement effective.

Le cas des détections heuristiques est plus délicat. Dans ce cas, le module écarté n'est pas réellement infecté et donc modifié, et le version du module que le processus de réparation va réinstaller est identique : l'antivirus (s'il est logique avec lui-même) va à nouveau écarter le module et la réparation est inexistante.

Comment détecter ce genre de cas :

- Après réparation, le processus de réparation vérifie qu'à ce moment l'installation est complète et intègre. Si, immédiatement après une réparation techniquement réussie, la vérification échoue, c'est que l'antivirus a écarté à nouveau le module, et le programme de réparation vous en avertira immédiatement
- Après réparation, le processus de réparation indique que la situation est en ordre. Mais lorsque vous redémarrez l'application, la vérification au démarrage (voir plus haut) indique à nouveau un problème, et surtout indique la disparition du **même** module que précédemment : l'antivirus est évidemment très suspect !
- Il n'est pas conseillé de travailler online sans antivirus. Pour confirmer ce type de situation, vous pouvez également :
  - Mettre l'ordinateur off-line et l'isoler de Internet
  - Arrêter l'antivirus
  - Exécuter la réparation off-line (voir plus haut)
  - Exécuter l'application : elle devrait fonctionner, puisque l'antivirus n'est plus là
  - Remettre l'antivirus en action : si l'application ne fonctionne à nouveau plus, l'antivirus est clairement impliqué

Si ce genre de cas est détecté, il faut configurer l'antivirus pour accepter ce module. Cette procédure dépend de l'antivirus et il n'est pas possible de la décrire ici pour tous les antivirus disponibles sur le marché : vous êtes renvoyés à la documentation de l'antivirus pour cette opération.

## **7 Outils disponibles**

- Corporate Desk :
  - Menu « aide », option « A propos de... »
    - Indication de la version et de la release de l'installation
    - Bouton « Détails » : carte d'identité de l'installation
  - Menu « Fichier », « Préférences », onglet « Internet »
    - Configuration des mises à jours automatiques
    - Possibilité de faire la mise à jour manuellement ou d'en importer une
- Panneau de configuration :
  - Option « Configuration détaillée de l'application » :
    - Carte d'identité de l'installation
    - Possibilité de faire la mise à jour manuellement ou d'en importer une
- Outil « CheckCDUUpdate »