

Cliquez sur la question qui correspond le mieux à votre inquiétude, et la réponse apparaîtra. Si vous n'êtes pas satisfait par cette réponse, vous pouvez nous contacter à travers [cette page](#) et nous vous répondrons au plus vite.

- [GÉNÉRAL - Qu'est-ce que Computrace Data Protection?](#)
- [GÉNÉRAL - Comment Computrace Localise et Protège un ordinateur à distance?](#)
- [GÉNÉRAL - Comment puis-je voir les informations sur mes actifs informatiques?](#)
- [GÉNÉRAL - Comment fonctionne Computrace?](#)
- [GÉNÉRAL - Qu'est que le programme ctmweb.exe livré avec Computrace?](#)
- [INSTALLATION: Comment puis-je contrôler que l'installation s'est faite correctement?](#)
- [ELIMINATION - Qu'est-ce que Data Deletion?](#)
- [ELIMINATION - Comment puis-je Pré-autoriser Data Delete pour mes actifs?](#)
- [ELIMINATION - Puis-je récupérer mes informations une fois effacées?](#)
- [ELIMINATION - Puis-je faire de l'élimination sélective?](#)
- [ELIMINATION - Comment puis-je m'assurer de la sécurité vis-à-vis des opérateurs?](#)

GÉNÉRAL - Qu'est-ce que Computrace Data Protection?

Computrace Data Protection offre deux avantages principaux: la gestion des biens informatiques (asset management) et la suppression des données à distance. Le produit est géré centralement par le département d'informatique (IT) et est destiné aux clients qui ont beaucoup d'utilisateurs d'ordinateurs soit à distance, soit qui sont mobiles. En ce qui concerne l'asset management des biens informatiques, Computrace Data Protection donne la possibilité au département IT de localiser jusqu'à 100% de leurs biens qui sont connectés (sur Internet), ceci incluant les 40% des biens qui sont, selon la Société Gartner, introuvables à un moment donné. La fonction « Data Delete » permet aux clients de supprimer à distance les données sensibles qui se trouvent sur les ordinateurs volés ou perdus. Data Delete peut également être utilisé pour garantir qu'il ne reste aucune information sensible sur un ordinateur à la fin de sa durée de vie.

GÉNÉRAL - Comment Computrace Localise et Protège un ordinateur à distance?

Chaque fois qu'un ordinateur se connecte sur Internet, Computrace Data Protection peut le localiser grâce à un minuscule agent de logiciel

(Computrace Agent), introuvable, implanté dans l'ordinateur. La localisation de l'ordinateur est envoyée au centre de surveillance (Monitoring Center) confidentiel et sûr d'Absolute. Le Computrace Agent peut également fournir des informations sur l'utilisateur, les équipements et logiciels qui aident l'entreprise à localiser et gérer leurs biens éloignés. En cas de vol d'un ordinateur, la fonction Data Delete peut être programmée, pour que les données sensibles soient supprimées dès que l'ordinateur appelle le Monitoring Center.

GÉNÉRAL - Comment puis-je voir les informations sur mes actifs informatiques?

: Les utilisateurs (normalement les départements IT) ont un accès à certains modules de la gestion des biens informatiques via le site Internet d'Absolute, dédié au service clients (« Customer Center »). Ces modules (ou rapports) permettent aux départements IT de mieux gérer la localisation des biens - Secure Asset Tracking.®

GÉNÉRAL - Comment fonctionne Computrace?

La technologie Computrace vous permet de localiser et gérer vos biens informatiques où qu'ils soient. Voilà comment :

Vous installez le logiciel client sur vos ordinateurs en utilisant l'installateur MSI, login scripts, imaging et d'autres méthodes de déploiement – c'est sûr et facile. Le logiciel client est petit, discret, et caché dans l'ordinateur. Chaque fois que vous vous connectez sur Internet, votre ordinateur donne votre localisation, nom d'utilisateur et les informations sur les logiciels et les équipements au Monitoring Center sécurisé d'Absolute.

Vous devez signer un accord de pré-autorisation afin d'activer la fonction de Data Delete sur le site Internet du « Customer Center ». Dans l'accord vous devez nommer les personnes autorisées d'exécuter Data Delete. Une fois qu'Absolute reçoit cette information, il envoie les clés « RSA SecurID® » aux personnes identifiées dans l'accord – les Data Delete Administrators. L'accord peut être téléchargé du site Customer Center – il se trouve dans le menu 'Data Delete'.

Vous pouvez localiser et gérer tous vos biens informatiques en utilisant les fonctions de rapport, alertes et administration qui se trouvent sur le site Customer Center.

En cas de vol, ou si l'ordinateur est à la fin de sa durée de vie ou à la fin de son contrat de location, vous pouvez vous servir de la fonction Data Delete pour supprimer toutes données sensibles afin de s'assurer que les informations ne tombent pas dans la main d'autrui. Seulement un Data Delete Administrator avec une clé RSA SecurID peut exécuter Data Delete.

GÉNÉRAL - Qu'est que le programme ctmweb.exe livré avec Computrace?

Ctmweb est un utilitaire permettant de paramétrer Computrace en cas de nécessité. Par exemple, il autorise la fonction d'appel manuel vers le serveur pour permettre une actualisation des informations.

Ctmweb n'est pas un programme nécessaire au fonctionnement de Computrace.

INSTALLATION: Comment puis-je contrôler que l'installation s'est faite correctement?

Si vous vous êtes assurés d'avoir une connexion internet active au moment de l'installation, Computrace se connectera au serveur pour s'identifier et informer de sa présence.

Le temps nécessaire pour que ces informations s'intègrent dans le [centre de monitoring](#) varie de 30 minutes à 1 heure.

Muni de votre login, vous pourrez ensuite voir apparaître votre ordinateur sur votre compte, avec ses informations de connexion et de configuration.

ELIMINATION - Qu'est-ce que Data Deletion?

La fonction de suppression des données (Data Delete) permet aux clients, en cas de vol ou perte d'un ordinateur, de supprimer à distance les données sensibles qu'il contient. En cas de vol d'un ordinateur, la fonction Data Delete peut être programmée, pour que dès que l'ordinateur appelle le Monitoring Center, les données sensibles soient supprimées. Data Delete peut également être utilisé pour garantir qu'il ne reste aucune information sensible sur un ordinateur à la fin de sa durée de vie ou à la fin d'un contrat de location.

ELIMINATION - Comment puis-je Pré-autoriser Data Delete pour mes actifs?

Les personnes ayant le pouvoir de signature doivent remplir et donner à Absolute un accord de pré-autorisation. (Renseignez-vous auprès de votre vendeur ou le télécharger sur le site Internet « Customer Center ». Il se trouve dans les rubriques « Data Delete » ou « Documentation ») . Une fois qu'Absolute reçoit cette information, il envoie les clés « RSA SecurID® » aux personnes identifiées dans l'accord – les Data Delete Administrators. Une fois que les clés sont reçues, Data Delete peut être installé sans l'intervention d'Absolute.

ELIMINATION - Puis-je récupérer mes informations une fois effacées?

Non, ce n'est pas possible de récupérer les données supprimées car la fonction utilise un algorithme au-dessus de la norme DOD5220.22-M défini par le Département de la Défense des Etats-unis pour la suppression des données et elle conforme avec la norme de NATO.

DOD5220.22-M est une norme définie par le Département de la Défense des Etats-unis pour la suppression des données qui garantie que toutes les informations anciennement encrustées sur les disques soient supprimer de manière permanente. En général, quand un ordinateur supprime un fichier, le contenu n'est pas vraiment supprimé – simplement le lien entre le fichier et le répertoire est coupé, mais les données restent dans les partitions (ou secteurs). Ces données y restent jusqu'à ce que l'ordinateur utilise à nouveau la partition en écrivant des nouvelles données. Tant que les données anciennes restent sur l'ordinateur il est possible de les récupérer en utilisant les programmes, comme les logiciels scientifiques, qui lisent directement les partitions de disques.

Même si un secteur est re-écrit le phénomène de « data remanence » (le résiduel physique qui démontre que les données ont été supprimées) peut permettre que les informations supprimées soient récupérées.

Pour être sûr qu'un fichier supprimé est vraiment supprimé il est nécessaire de re-écrire tous les secteurs d'information de ce fichier. Il ne suffit pas de simplement supprimer ou « formater » le disque car il existe beaucoup d'outils capables de récupérer les données « perdues. »

Cette norme oblige à ce que chaque partie du magnetic media device soit écrit 3 fois ; premièrement en donnant une valeur fixe (0x00) puis sa valeur complémentaire (0xff) une fois, et ensuite une fois avec des valeurs faites au hasard. L'algorithme du Data Delete d'Absolute dépasse cette norme car il re-écrit les données 7 fois (au lieu de 3 fois) et en exécutant d'autres opérations supplémentaires. L'algorithme re-écrit la cible 7 fois – les 6 premières fois en utilisant les 1 et les 0 en alternation et puis la dernière fois il écrit une valeur au hasard.

Ecrit des données au hasard sur le fichier

Change les attributions du fichier au « répertoire »

Change le fichier heure/date pour une valeur fixe

Règle la taille du fichier au « 0 »

Change le nom du fichier pour un autre qui est choisi au hasard

Enlève le nouveau nom du répertoire

ELIMINATION - Puis-je faire de l'élimination sélective?

Actuellement Data Delete propose 3 niveaux de suppression de données :

- Suppression des fichiers ou répertoires spécifiques – (uniquement pour PC). L'utilisateur peut choisir les fichiers, types de fichiers et/ou répertoires qu'il souhaite supprimer. L'ordinateur restera opérationnel après le processus de Data Delete si l'utilisateur n'a pas supprimé les répertoires d'exploitation (OS). Par exemple, il est possible de choisir de supprimer tous les fichiers dans le répertoire « Mes Documents » et tous les documents Word, Excel, Powerpoint et PDF où qu'ils se trouvent dans l'ordinateur. Pour pouvoir utiliser cette option il est nécessaire de créer une police de Data Delete qui se trouve dans le menu Administration->Data Delete.
- Suppression totale des données sauf le système d'exploitation – Tous les fichiers sauf les fichiers du système d'exploitation (OS) sont supprimés du disque dur – l'ordinateur restera opérationnel après le processus de Data Delete.
- Suppression totale des données y compris le système d'exploitation (OS) – Tous les fichiers qui ne sont pas du système d'exploitation et quelques fichiers du système d'exploitation sont supprimés du disque dur. Tous les fichiers (y compris les programmes et données) seront supprimés ainsi que quelques fichiers du système d'exploitation pour éviter que l'ordinateur ne démarre. Quelques fichiers du système d'exploitation resteront sur l'ordinateur. L'ordinateur ne sera plus opérationnel après le processus de Data Delete.

En cas d'une suppression complète y compris les fichiers OS, le processus de Data Delete s'opère en deux phases – Premièrement tous les fichiers sauf ceux OS sont supprimés, un fichier comprenant tous les noms des fichiers supprimés est téléchargé (au Monitoring Center) et la suppression des fichiers OS est lancée. L'Agent Computrace ne peut pas appeler (le Monitoring Center) une fois que la suppression est en cours d'exécution donc le Data Delete est programmé comme « terminé » une fois que la suppression des fichiers non OS est exécutée.

ELIMINATION - Comment puis-je m'assurer de la sécurité vis-à-vis des opérateurs?

: Il existe plusieurs moyens de vérification et d'authentification afin de s'assurer que seules les personnes autorisées par la société puissent lancer le Data Delete. Premièrement l'entreprise spécifie dans un accord de pré-autorisation les personnes autorisées pour lancer Data Delete (« Data Delete Administrators »). Ensuite, ces personnes autorisées reçoivent une clé RSA SecurID. Pour lancer le Data Delete depuis le Customer Center, le Data Delete Administrator se connecte et ouvre la fenêtre correspondante à la demande de suppression des données, il sélectionne l'ordinateur ainsi que les options du Data Delete, ensuite rentre le code de sa clé RSA SecurID (ce code change toutes les 60 secondes) et enfin il entre à nouveau le mot de

passer du Customer Center pour valider la demande de Data Delete.

En résumé, les moyens de sécurité suivants sont en place pour éviter la suppression de données non autorisée :

Un accord original de pré-autorisation aura dû être rempli, signé et envoyé à Absolute pour pouvoir accéder à la fenêtre de demande de suppression des données dans le Customer Center.

Il est obligatoire que la personne connectée au Customer Center soit un Data Delete Administrator autorisé et identifié dans l'accord de pré-autorisation.

La personne connectée doit avoir les accès d'administrateur dans le Customer Center.

Il est obligatoire que cet utilisateur ait en sa possession de la clé RSA SecurID d'Absolute. Cette clé est nominative et ne peut pas être échangée avec un autre utilisateur ou un autre compte.

Le mot de passe rentré à l'écran pour la demande de suppression des données doit être le même que celui de l'utilisateur connecté au Customer Center.

Le code (chronométré) qui se trouve sur la clé RSA SecurID et qui est rentré à l'écran de la demande de Data Delete doit être le même que celui qui se trouve sur le serveur SecurID d'Absolute attribué à l'utilisateur spécifique du Customer Center.

Si toutes les conditions ci-dessus sont remplies, le Data Delete sera prêt à être lancé dès que l'ordinateur se connecte sur Internet. En plus de tous ses moyens de sécurité, un e-mail est envoyé aux personnes qui ont signé l'accord de pré-autorisation une fois que le Data Delete est demandé, lancé et terminé.
