



Guide de démarrage rapide



Welcome

Vous êtes l'administrateur référent du système d'information de votre entreprise et vous avez la charge de la protection des données de vos utilisateurs.

Ce guide est fait pour vous, vous découvrirez ici les essentiels de la prise en main de votre compte administrateur, jusqu'à votre première restauration...

Bravo & Bienvenue à bord, vos données sont entre de bonnes mains 😊



5 minutes

Pour tout comprendre...

Sommaire

1

Activer son
compte
administrateur

5

Créer sa
première
sauvegarde

unyc Rejoignez l'aventure

2

Créer les
utilisateurs

6

Restaurer une
sauvegarde

3

Installer son 1er
agent de
sauvegarde

7

Liens utiles...

4

Créer le plan de
protection

8

Annexe
Prérequis
Parefeu

1 Ma première connexion Administrateur

Après réception du mail d'activation (il se cache parfois dans vos courriers indésirables 😊), il vous suffit de cliquer sur « Activer votre compte »...

Vous serez redirigé automatiquement sur votre plateforme Cyberbackup et devrez définir le mot de passe de votre compte administrateur.

Le tour est joué ! Conservez précieusement **votre ID** et **sésame** de connexion.

Votre plateforme [cyber.backup.unyc.io](https://www.cyber.backup.unyc.io) est désormais accessible



2 Création des utilisateurs

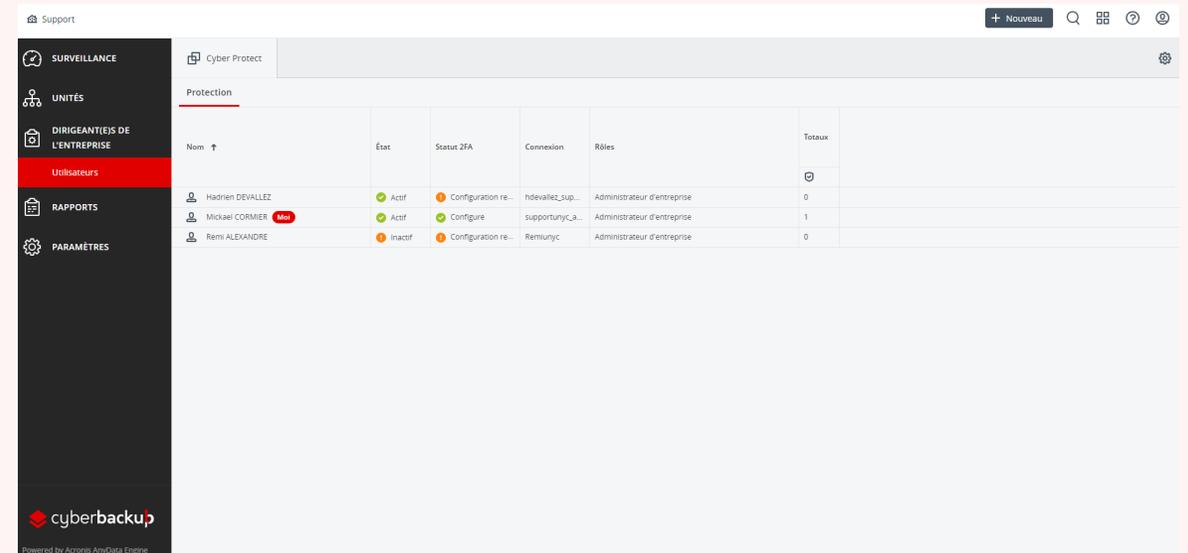
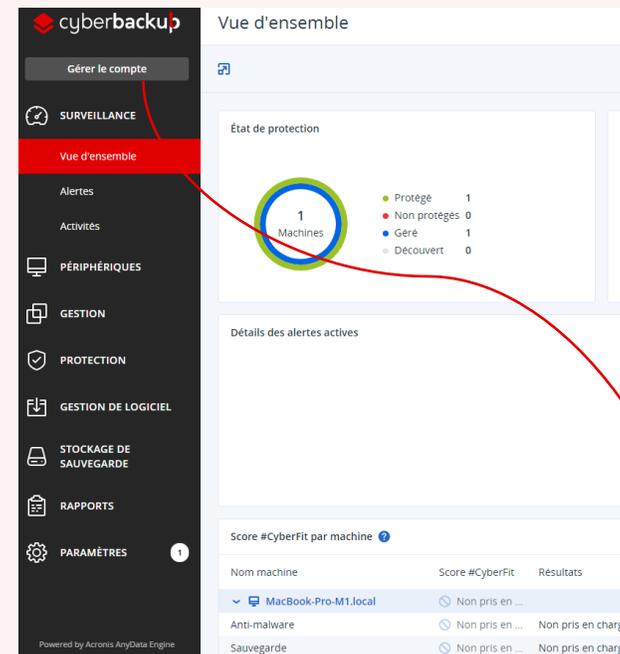
Maintenant que vous disposez de votre accès administrateur. Il est temps de créer vos utilisateurs :

- Rendez vous dans la section « Gérer le compte » puis utilisateurs.
- Cliquez sur « + Nouveau »
- Complétez les infos utilisateurs

Chaque utilisateur doit disposer d'un « rôle » (tous les détails des permissions permettant de réaliser des actions précises ... [plus d'infos](#))

- Utilisateur
- Administrateur en lecture seule
- Administrateur
- Opérateur de restauration

Une fois vos utilisateurs déclarés, il ne reste plus qu'à leur associer des périphériques et les plans de protection adéquates.



3 Premiers pas depuis un périphérique utilisateur

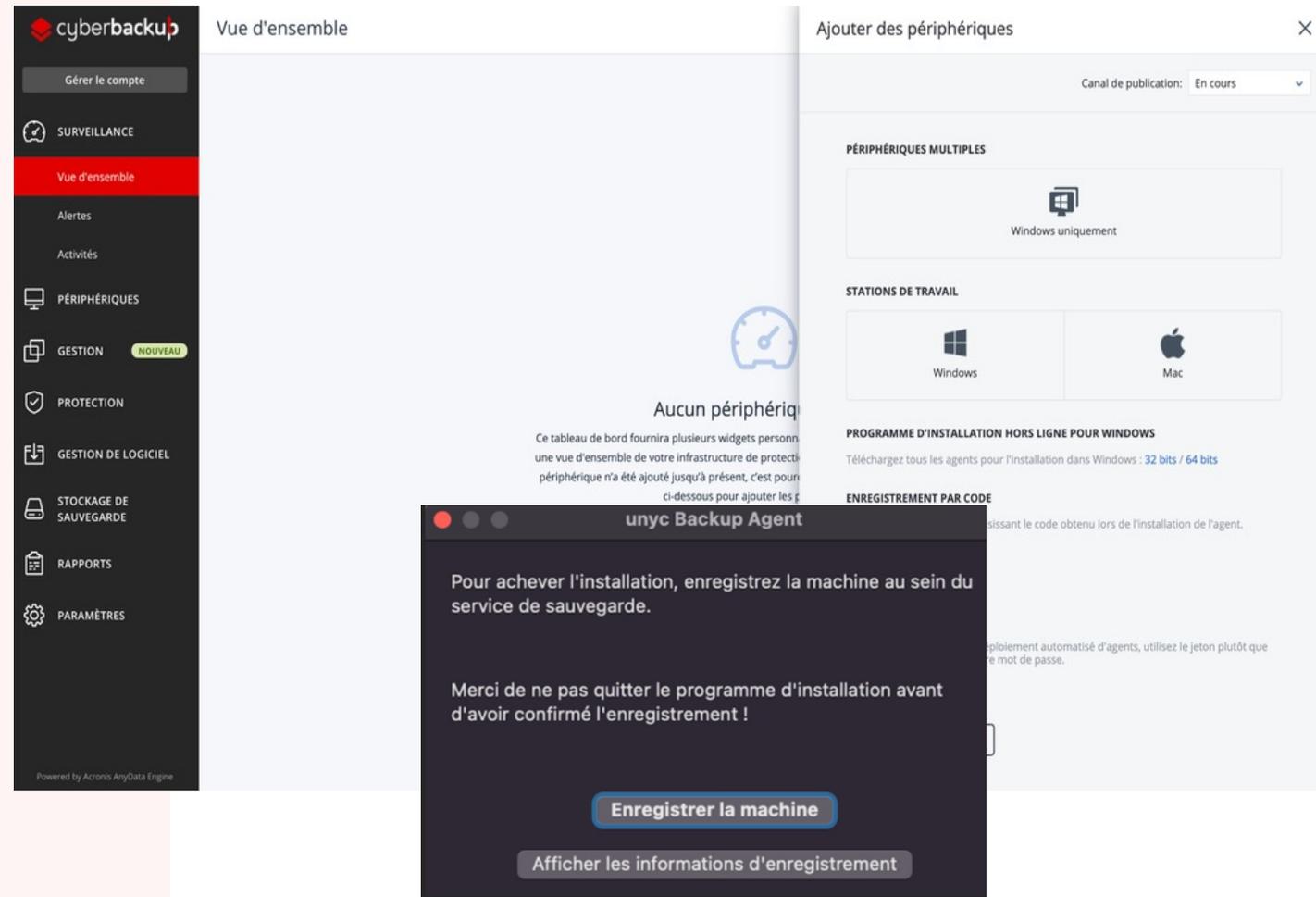
Nous y sommes !

Vous allez déployer votre 1er agent de sauvegarde sur un poste utilisateur.

Que faire :

- Ouvrir la machine client en mode administrateur
- Se rendre sur le portail cyber.backup.unyc.io et se connecter avec son compte admin.
- Depuis la section vue d'ensemble, cliquez sur « Ajouter des périphériques », Téléchargez et installez l'agent pour le poste client (Mac ou Windows)
- Une fois terminé, le programme d'installation vous demandera d'enregistrer le poste de travail... Suivez le guide
- Il vous reste à associer le périphérique au bon utilisateur depuis le menu périphérique

Votre poste client est opérationnel 👍



4 Créer un plan de protection

Dans le menu "Plan de protection", cliquez sur "+ Création d'un plan" pour commencer.

Vous pouvez effectuer **les actions suivantes** :

- Renommer le plan
- Activer ou désactiver un module du plan de protection
- Configurer un module en cliquant dessus pour l'agrandir, puis en modifiant les paramètres selon vos besoins.
- Sélectionner les postes de travail auxquels appliquer le plan de protection en cliquant sur "Ajouter des périphériques".

Pour finaliser la création du plan de protection, cliquez sur le bouton "Créer". [Plus d'info...](#)

The screenshot shows the Cyberbackup web interface. On the left is a dark sidebar with the Cyberbackup logo and a menu with items: 'Gérer le compte', 'SURVEILLANCE', 'PÉRIPHÉRIQUES', 'GESTION' (with a 'NOUVEAU' tag), 'Plans de protection' (highlighted in red), 'Plans de l'agent' (with a 'NOUVEAU' tag), 'Réplication de MV', 'PROTECTION', 'GESTION DE LOGICIEL', 'STOCKAGE DE SAUVEGARDE', 'RAPPORTS', and 'PARAMÈTRES'. At the bottom of the sidebar, it says 'Powered by Acronis AnyData Engine'. The main content area is titled 'Plans de protection' and has a '+ Création d'un plan' button in the top right corner, which is pointed to by a red arrow. Below this is a 'Créer un plan de protection' section with a sub-header 'Le plan de protection contient un ensemble de fonctionnalités qui répondent à différents besoins : sauvegarde et bien plus.' and two links: 'Comment créer un plan de protection' and 'En savoir plus'. A modal window titled 'Créer un plan de protection' is open, showing a form for creating a new plan. The form has a title 'Nouveau plan de protection (1)' and buttons for 'Annuler' and 'Créer'. The form includes several sections: 'Sauvegarde' (toggle on), 'Quoi sauvegarder' (dropdown: 'Toute la machine'), 'Où sauvegarder' (dropdown: 'Stockage sur le Cloud'), 'Planification' (dropdown: 'Lundi à vendredi à 16:15'), 'Durée de conservation' (dropdown: 'Mens.: 6 mois, Hebdo.: 4 semaines, Journ.: 7 jours'), 'Chiffrement' (toggle on, 'Spécifier un mot de passe'), 'Sauvegarde d'applications' (dropdown: 'Désactivé'), 'Options de sauvegarde' (button: 'Changer'), 'Protection contre les virus et les malware' (toggle on, 'Autoprotection activée'), 'Évaluation des vulnérabilités' (toggle on), and 'Contrôle du périphérique' (toggle on, 'L'accès à tous les périphériques est autorisé. Les listes d'autorisation sont config...').

5 Créer sa première sauvegarde

Votre plan de protection contient une brique paramétrable liée à la configuration des sauvegardes

Depuis celle-ci, vous pouvez effectuer **les actions suivantes** :

- Quoi Sauvegarder (tout ou partie)
- Ou sauvegarder
- Fréquence et périodicité de sauvegarde
- Chiffrement avec ou sans mot de passe

La sauvegarde se lancera automatiquement en fonction de la périodicité définie.

A tout moment, depuis le menu « Tous les périphériques », vous pouvez lancer **une sauvegarde manuelle** d'un périphérique en cliquant sur « Sauvegarder maintenant ».

Créer un plan de protection

Ajouter des périphériques

Nouveau plan de protection (3) [Annuler] [Créer]

Sauvegarde
Toute la machine a Stockage sur le Cloud, Lundi à vendredi à 17:30 (Toujours incr...

Quoi sauvegarder: Toute la machine

Où sauvegarder: Stockage sur le Cloud

Planification: Lundi à vendredi à 17:30 (Toujours incrémentielle)

Durée de conservation: Mens.: 6 mois, Hebdo.: 4 semaines, Journ.: 7 jours

Chiffrement Spécifier un mot de passe

Sauvegarde d'applications: Désactivé

Options de sauvegarde: Changer

Protection contre les virus et les malware: Autoprotection activée

Évaluation des vulnérabilités: Packages Linux, produits Microsoft, produits Windows tiers, produits Apple, prod...

Contrôle du périphérique: L'accès à tous les périphériques est autorisé. Les listes d'autorisation sont config...

unyc2109mac194-1.home

Etat: Sauvegarde planifiée

Dernière sauvegarde: —

Prochaine sauvegarde: 24 Mars 2023, 17:01

[SAUVEGARDER MAINTENANT] [RESTAURER]

plan de protection

Powered by Acronis AnyData Engine

Nb chiffrement des sauvegardes : Vous serez invité à activer le chiffrement pour garantir et sécuriser vos sauvegardes . Nous vous encourageons à le faire.

⚠ A Noter, si vous ajoutez un mot de passe de chiffrement, le support technique unyc ne pourra pas intervenir en cas d'oubli. Pensez à bien le conserver !

6 Restaurer une sauvegarde

Depuis la rubrique « Tous les périphériques », vous trouverez l'ensemble des postes sauvegardés. Il est possible de lancer une **restauration**.

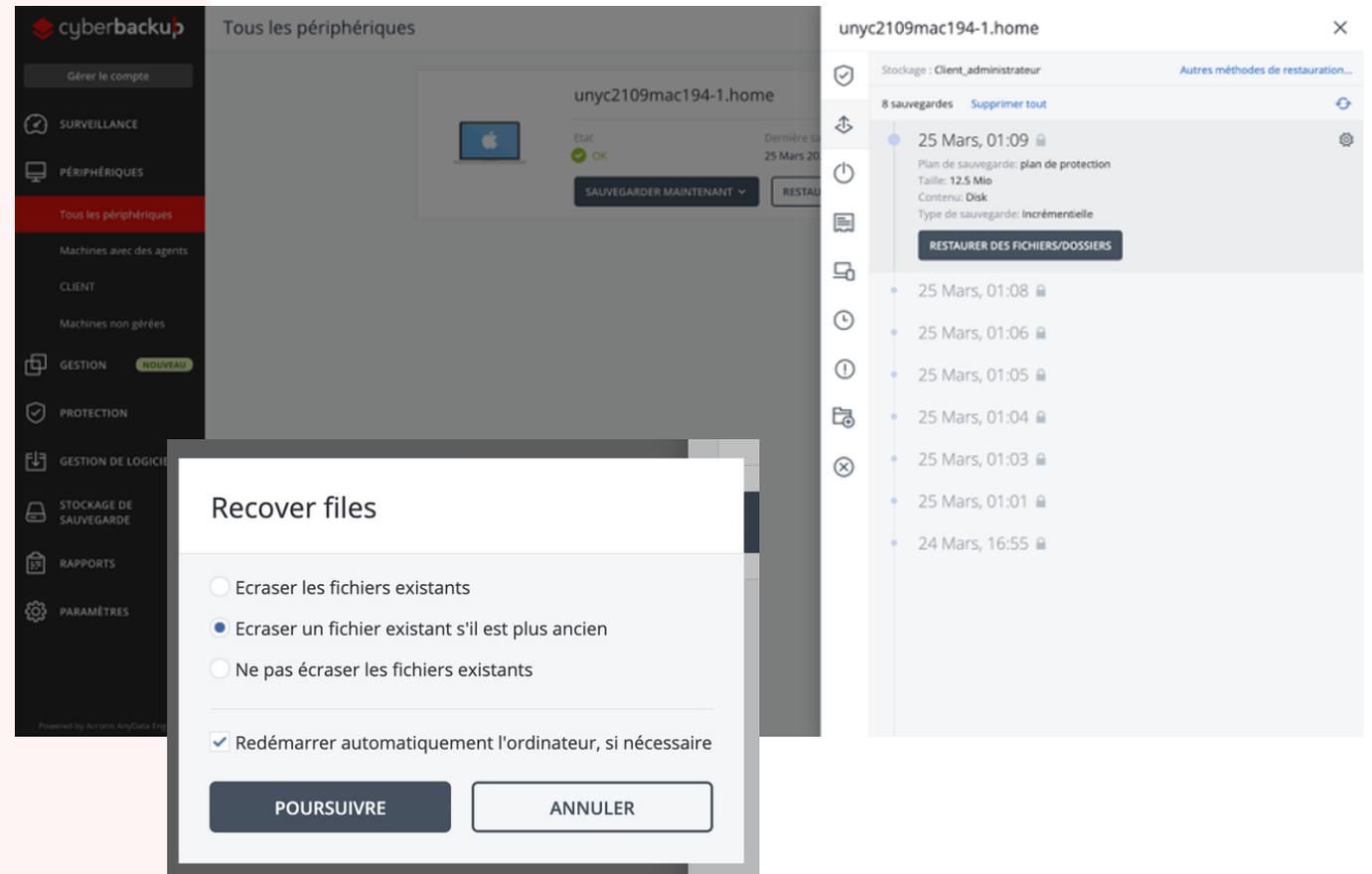
Deux possibilités en fonction de votre plan de protection mise en place :

- Soit lancer une restauration de fichier/dossier
- Soit lancer une restauration complète de poste

N'oubliez pas de définir le « chemin d'accès » de la restauration à son emplacement d'origine ou vers un emplacement personnalisé.

Vos données sont de nouveau disponibles 😊

unyc Rejoignez l'aventure



Nb Sauvegardes chiffrés: ⚠️ Si vous ne disposez plus du mot de passe de déchiffrement de vos sauvegardes, celles-ci seront inutilisables et peuvent être considérées comme perdues.

Merci pour votre installation

Pour plus de détails :

Vous pouvez vous référer à notre site de [ressources en ligne](#) 



Annexe

Préréquis Parefeu

Assurez-vous que le pare-feu et les autres composants du système de sécurité de votre réseau (comme un serveur proxy) autorisent les connexions sortantes via les ports TCP suivants :

- Ports **443** et **8443**

Ces ports permettent d'accéder à la console de service, d'enregistrer des agents, de télécharger des certificats, d'autoriser des utilisateurs et de télécharger des fichiers depuis le stockage dans le cloud.

- Ports entre **7770** et **7800**

Ces ports permettent aux agents de communiquer avec le serveur de gestion.

- Ports **44445** et **55556**

Ces ports permettent aux agents de transférer des données lors du processus de sauvegarde et de restauration.

