



Splashtop Enterprise

Guide d'administrateur

03 novembre 2022

Table des matières

Journal des modifications - par rapport à la dernière version du 20/04/2022	4
1. Déploiement.....	5
Comment mettre à jour Splashtop Streamer ?	9
Politiques de préférences.....	10
2. Exigences supplémentaires pour MacOS	11
3. Signature unique (SSO).....	12
4. Inviter des utilisateurs.....	13
Rôles de l'équipe	13
5. Groupement.....	15
Ajouter des utilisateurs ou des ordinateurs à un groupe	16
6. Autorisations d'accès.....	17
7. Accès programmé.....	19
Configuration de l'Accès Programmé	19
Gestion des ressources et programmes	24
Si un administrateur de groupe est supprimé, qu'advient-il de ses ressources/programmes ?	25
8. Paramètres d'équipe	26
Aperçu des paramètres d'équipe.....	26
9. Contrôles granulaires	29
10. Gestion des ordinateurs à distance (techniciens).....	31
Journaux des événements Windows	31
Inventaire informatique – Système, matériel, logiciel.....	31
Sécurité des points terminaux	32
Mises à jour Windows.....	32
Actions 1-to-Many et calendriers	33
Alertes configurables	34
Commande à distance	34
11. Accès avec surveillance - SOS (techniciens).....	35
Paramètres granulaires.....	35
12. Personnalisation de SOS (techniciens).....	36

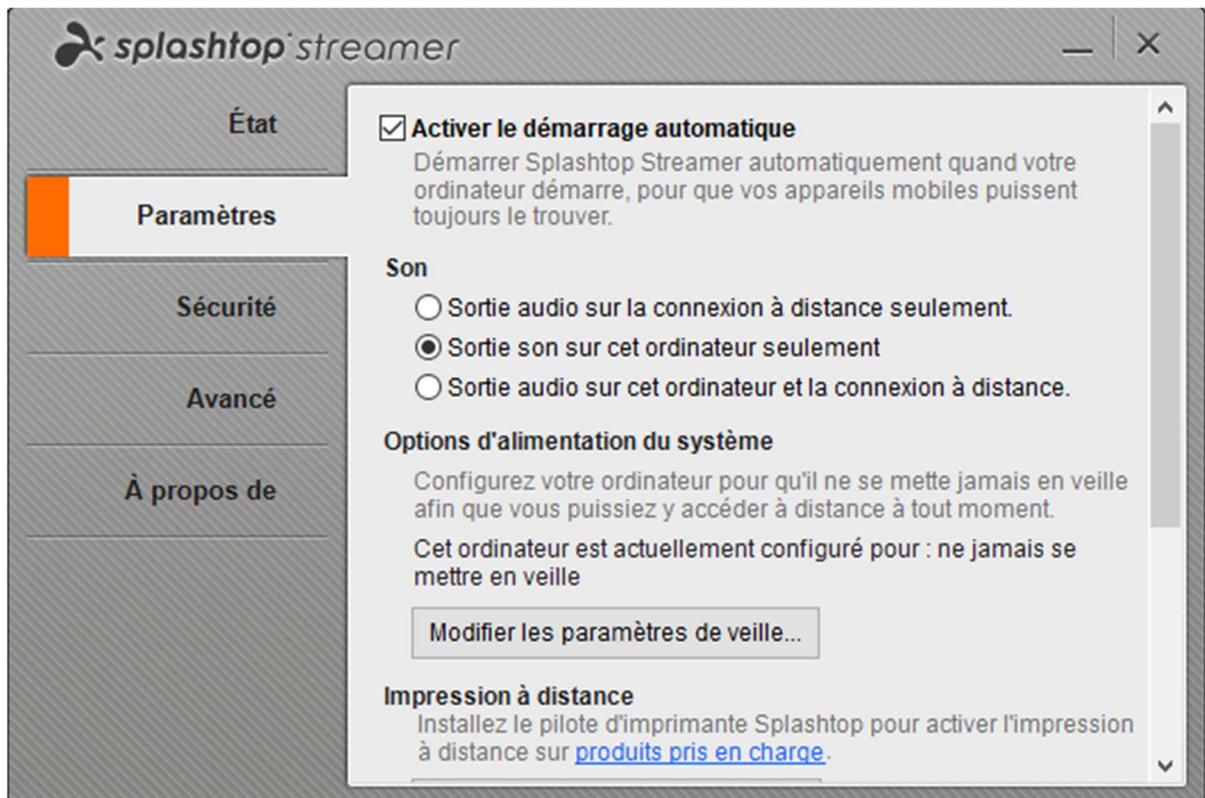
13.	Service Desk (techniciens).....	38
14.	LOGS.....	39
15.	Fonctionnalités supplémentaires	40
	Restriction IP	40
	Création de journaux SIEM	40
	Splashtop Connector.....	41
	Splashtop AR	41

Journal des modifications - par rapport à la dernière version du 20/04/2022

- Déploiement, Section 1
 - Ajout de politiques de préférence, pour la gestion des paramètres de streamer et de session à partir de la console Web
- Inviter des utilisateurs, Section 4
 - Révision et ajout d'informations sur les super administrateurs
- Contrôles granulaires, section 9
 - Ajout de 1-to-Many à la liste des contrôles granulaires pris en charge
- Gestion d'ordinateur à distance, Section 10
 - Ajout d'informations sur le tableau de bord Inventaire
 - La modification d'informations pour les scripts 1-to-many est maintenant inclus par défaut dans les licences Technicien.
- Ajout de la section 13, Service Desk
 - Ajout d'une mention pour code PIN à 6 chiffres

1. Déploiement

Installez Splashtop Streamer sur les ordinateurs pour les rendre accessibles à distance. Vous pouvez créer un paquet de déploiement pour [personnaliser les paramètres de déploiement du Streamer](#). Cela vous permettra de ne pas avoir à configurer manuellement les paramètres après l'installation.



[Aperçu des différents paramètres du Streamer](#)

1. Connectez-vous à my.splashtop.com et cliquez sur **Gestion -> Déploiement**.



2. Cliquez sur **Créer un paquet de déploiement** et sélectionnez les paramètres du Streamer souhaités. Lors de la création du paquet de déploiement, vous avez la possibilité de spécifier les paramètres par défaut, y compris la règle de nommage de l'ordinateur, les paramètres de sécurité, la redirection du son, etc.

Réglages généraux

Lancer automatiquement Streamer

Lancez automatiquement Splashtop Streamer à chaque démarrage de l'ordinateur.

Délai d'expiration de session inactive

Les sessions à distance se déconnecteront automatiquement après minutes sans activité (0 signifie jamais expiré).

Masquer l'icône de plateau

Masquer l'icône Streamer sur la barre d'état système Windows ou la barre de menus Mac. Cochez cette option pour réduire le risque que les utilisateurs falsifient Streamer.

Activer la connexion directe

Lorsque vous êtes sur le même réseau, utilisez une connexion directe pour de meilleures performances. En fonction de la politique de sécurité de votre organisation, vous souhaitez peut-être désactiver cette option.

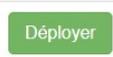
Sécurité

Nécessite une authentification Windows ou Mac

Exigez la saisie du nom d'utilisateur et du mot de passe de

Remarque : Si vous utilisez l'authentification unique (SSO), ne sélectionnez pas « Verrouiller les paramètres du streamer en utilisant les identifiants d'administration Splashtop », car les comptes SSO ne peuvent pas déverrouiller le streamer.

3. Après avoir sauvegardé le paquet, vous pouvez voir le paquet nouvellement créé et le code de déploiement unique à 12 chiffres. Cliquez sur **Déployer** pour voir les options de déploiement.

Nom du package de déploiement	Règle de nommage d'ordinateur	Code	Date de Création	Déployer
Animation	Utiliser le nom de l'ordinateur actuel	PY42WJK2WPXS	202 	

4. Vous trouverez deux options pour distribuer le paquet de déploiement :

Option 1 : Partager le lien

Envoyez ce lien pour permettre à un utilisateur de télécharger et d'installer le Streamer pour vous.

Lien partageable

https://my.splashtop.com/team_deployment/download/PY42WJK2WPXS

Essayez le lien

Option 1: Partager le lien

- 1 Envoyez le lien ci-dessus à vos utilisateurs. Le lien les mènera à une page Web où ils pourront télécharger l'installateur et suivre des instructions simples pour la configuration.
- 2 Une fois que vos utilisateurs ont exécuté le programme d'installation, leurs ordinateurs seront accessibles par vous.

Les utilisateurs qui suivront le lien verront les instructions pour télécharger et installer le streamer.

Bienvenue à Splashtop Remote Support

Installez Splashtop Streamer sur votre ordinateur pour permettre à l'organisation ci-dessous d'accéder à distance à votre ordinateur à tout moment (sauf configuration contraire).

[redacted]'s team (owner: [redacted]@splashtop.com)

Je fais confiance à l'organisation ci-dessus et souhaite autoriser l'accès à distance à mon ordinateur.

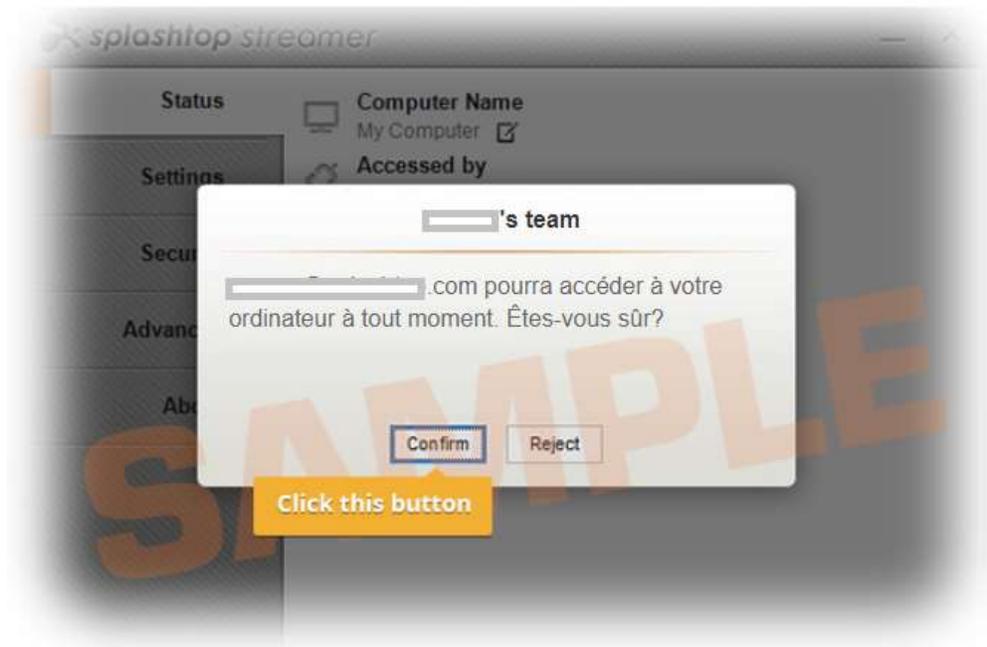
Étape 1: Téléchargez Streamer



Aussi disponible pour  Mac,  Android

Étape 2: exécutez le programme d'installation et autorisez l'accès

Une fois l'installation terminée, ouvrez l'application Streamer Splashtop et cliquez sur «Confirmer» pour autoriser l'accès.



Option 2 : Télécharger l'installateur

Téléchargez le programme d'installation pour effectuer l'installation directement sur votre ordinateur, partager via Dropbox, par e-mail, etc. ou préparer le déploiement avec un outil tiers.

Option 2: Télécharger l'installateur

Plateforme   

Windows (EXE, version 3.4.6.0) (Déploiement facile) ▼

Télécharger



Installateur de déploiement facile : le code de déploiement est intégré au programme d'installation. Il n'est pas nécessaire de saisir le code de déploiement lors de l'installation de Streamer.

- 1 Téléchargez le programme d'installation de Streamer.
- 2 Envoyez l'installateur et le code à 12 chiffres à vos utilisateurs.
- 3 Une fois que vos utilisateurs ont exécuté le programme d'installation et entré le code, leurs ordinateurs seront accessibles par vous.

Plusieurs installateurs sont proposés pour Windows, Mac, Android et Linux.

- Consultez cet article pour voir les [paramètres d'installation silencieuse](#)
- Des guides de déploiement sont également disponibles pour:
 - [Group Policy \(GPO\)](#)
 - [Jamf Pro](#)
 - [Microsoft Intune](#)
- Les paramètres du paquet de déploiement ne s'appliquent au Streamer qu'au moment de l'installation. Pour mettre à jour les paramètres d'un Streamer après le déploiement, vous pouvez le redéployer avec un nouveau paquet ou modifier manuellement les paramètres directement dans le Streamer.
- La suppression d'un paquet de déploiement n'affecte pas les ordinateurs déjà déployés, elle empêche tout nouveau déploiement avec le code de ce paquet.

Comment mettre à jour Splashtop Streamer ?

Il existe plusieurs façons de mettre à jour le Streamer :

- Mise à jour manuelle à partir de la console Web
- Mise à jour manuelle à partir de Streamer -> À propos de -> onglet Rechercher des mises à jour
- Mise à jour manuelle en exécutant le dernier programme d'installation du Streamer
- Mise à jour silencieuse au moyen des fichiers .EXE, .MSI ou .PKG

Pour plus d'informations, consultez cet article sur [la mise à jour de Splashtop Streamer](#).

Politiques de préférences

À partir de Splashtop Streamer v3.5.2.2, vous pouvez gérer certains paramètres de streamer et de session depuis la console Web via les politiques de préférences. En affectant des terminaux à votre politique, vous pouvez configurer et remplacer les paramètres existants du Streamer sans avoir à le redéployer ou à modifier manuellement les paramètres au niveau du terminal.

1. Pour créer une nouvelle politique, connectez-vous à my.splashtop.com et cliquez sur **Gestion** -> **Politique de préférences**.
2. Ajoutez ou supprimez différents paramètres de la politique, notamment les paramètres généraux de session, de sécurité et de bande passante.
3. Affectez des ordinateurs à la politique.
Remarque : seuls les streamers v3.5.2.2+ seront affichés dans le menu.
4. Les ordinateurs affectés seront marqués par une nouvelle icône qui indique qu'ils font partie d'une politique.
5. Lorsqu'un utilisateur se connecte à un ordinateur relevant de votre politique de préférences, les paramètres ou restrictions configurés s'appliquent à la session à distance. L'utilisateur ne pourra pas reconfigurer les paramètres de la politique à partir des menus de l'application Business ou du Streamer.

[Consultez cet article pour en savoir plus sur le fonctionnement et les instructions.](#)

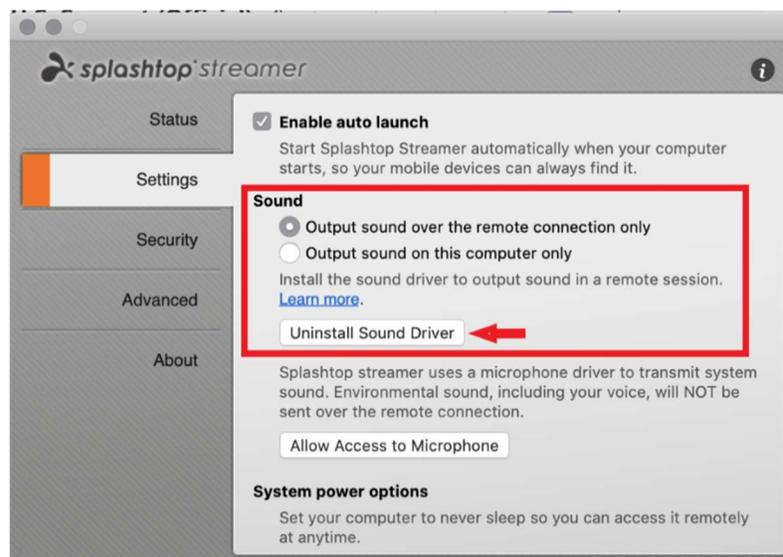
2. Exigences supplémentaires pour MacOS

En cas de déploiement sur des ordinateurs Mac, prenez note de ces exigences et instructions de configuration supplémentaires :

- **Autorisations de sécurité et de confidentialité** pour macOS [10.14 Mojave](#) , [10.15 Catalina / 11 Big Sur](#) et les versions plus récentes :



- **Audio** : Pour permettre la diffusion audio en continu sur la connexion à distance, [installez le pilote audio Splashtop](#) et autorisez l'accès au microphone pour Mojave/Catalina/Big Sur. Si des applications sur les ordinateurs Mac utilisent des pilotes audio tiers, tels que Avid Pro Tools ou Adobe Premiere, certaines [configurations supplémentaires](#) peuvent être nécessaires.



3. Signature unique (SSO)

Splashtop permet de se connecter à <https://my.splashtop.com> et à l'application Splashtop Business en utilisant les identifiants créés par vos fournisseurs d'identité SAML 2.0.

Si vous souhaitez que les utilisateurs utilisent le Single Sign-On (SSO), veuillez suivre les deux étapes suivantes :

1. Créez une méthode d'authentification unique (SSO) pour votre service IDP dans la console Web Splashtop:
Comment demander une nouvelle méthode d'authentification unique ?
 - a. Vous trouverez des instructions détaillées sur certains services IDP, tels qu'Azure AD, OKTA, ADFS, JumpCloud, OneLogin, ici :
[Ouverture de session unique \(SSO\)](#)
2. Notre équipe de validation vous contactera avec des instructions pour vérifier votre accès au domaine et activer votre méthode SSO.
3. (Recommandé) Configurez le **provisionnement SCIM** (pour [AzureAD](#), [Okta](#) et [JumpCloud](#)) pour provisionner et synchroniser automatiquement les utilisateurs et les groupes. Cela permet de passer outre le processus d'invitation par e-mail (*Section 4, Inviter des utilisateurs*).
4. (Recommandé) [Si vous ne pouvez pas à utiliser le provisionnement SCIM, importez les utilisateurs SSO au moyen d'un fichier CSV](#) pour intégrer automatiquement les utilisateurs dans certains groupes d'utilisateurs. Cela permet également de passer outre le processus d'invitation par e-mail.

[Consultez cet article pour découvrir les limites du SSO.](#)

Une fois votre méthode SSO activée, notez que vous pouvez désactiver l'[Authentification des appareils](#) pour les utilisateurs qui sont associés à cette méthode. De cette façon, les utilisateurs n'ont pas besoin de cliquer sur des liens d'e-mails supplémentaires pour authentifier leurs appareils. Il suffit de décocher la case Authentification des appareils de la méthode SSO sous **Gestion -> Paramètres (propriétaire d'équipe uniquement)** .

Par défaut (réinitialiser)	Statut	Nom SSO	IDP Type	Protocole	Authentification de l'appareil	Paramètres
<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="text"/>	ADFS	SAML 2.0	<input type="checkbox"/>	

4. Inviter des utilisateurs

Invitez les utilisateurs en allant sur **Gestion -> Utilisateurs -> Inviter des utilisateurs**. Attribuez les rôles d'équipe, les groupes d'utilisateurs et les méthodes d'authentification SSO pendant le processus d'invitation ou plus tard. Vous pouvez inviter jusqu'à 500 adresses e-mail dans chaque fenêtre d'invitation.

Inviter des utilisateurs par e-mail X

Email

Vous pouvez entrer plusieurs adresses électroniques. Séparez-les par une virgule ou mettez-en une par ligne.

Rôle : Admin Groupe Groupe par défaut

Définir en tant qu'administrateur spécifique au groupe au lieu d'administrateur ordinaire

* Les administrateurs peuvent accéder à tous les ordinateurs par défaut. Les membres ne peuvent accéder à aucun ordinateur par défaut. Vous pouvez utiliser "Autoriser l'accès" ou "Attribuer un groupe" pour modifier l'autorisation d'accès ultérieurement.

Méthode d'authentification

Rôles de l'équipe

- **Propriétaire** : le propriétaire est le plus haut niveau d'autorité et peut exécuter toutes les fonctions de Splashtop, notamment (mais sans s'y limiter) inviter des utilisateurs, modifier les rôles, consulter l'historique des connexions de chacun, gérer les ordinateurs, modifier les autorisations d'accès et changer les paramètres de l'équipe. Le propriétaire de l'équipe est le seul utilisateur qui a accès aux informations relatives à l'abonnement et à la facturation de l'équipe.
 - Il n'y a qu'un seul propriétaire, et le statut ne peut pas être transféré entre les comptes utilisateur.

- **Administrateur** : Le rôle d'administrateur a les mêmes autorisations que le propriétaire ci-dessus, sauf qu'il ne peut pas accéder aux informations d'abonnement et de paiement, à l'onglet Paramètres d'équipe et ne peut pas modifier les rôles des utilisateurs.
 - [Super administrateur](#) : le super administrateur est un rôle supérieur à celui d'administrateur, et peut avoir les mêmes autorisations que le propriétaire ci-dessus, notamment accéder à l'onglet Paramètres d'équipe et modifier le rôle des utilisateurs. Il ne peut pas accéder aux informations d'abonnement/de facturation.
 - [Administrateur de groupe](#) : Le rôle d'administrateur de groupe est un rôle d'administrateur limité qui donne à un utilisateur des privilèges d'administrateur sur des groupes d'utilisateurs et/ou d'ordinateurs spécifiques. Il permet d'ajouter/supprimer des utilisateurs et ordinateurs uniquement pour les groupes autorisés.
 - Les administrateurs et les administrateurs de groupe ont accès aux fonctionnalités de gestion à distance (commande à distance, inventaire du système, etc.) si vous avez acheté des **licences Technicien** de Splashtop Enterprise. Il sera bientôt possible de déléguer à certains utilisateurs l'accès à ces fonctionnalités (quel que soit leur rôle au sein de l'équipe).

- **Membre** : Les membres sont des utilisateurs génériques qui ont été ajoutés à l'équipe pour bénéficier d'un accès à distance. Ils n'ont accès qu'aux ordinateurs pour lesquels ils ont reçu une autorisation et peuvent vérifier leur propre statut, leurs informations de compte, les informations sur l'équipe et les journaux. Ils peuvent se retirer (« quitter ») d'une équipe dans l'onglet Résumé du compte.

5. Groupement

Avec Splashtop, vous pouvez regrouper vos utilisateurs et vos ordinateurs pour faciliter la gestion et le contrôle des autorisations d'accès. Chaque utilisateur ou ordinateur ne peut appartenir qu'à un seul groupe. Toutefois, les utilisateurs peuvent avoir accès à plusieurs groupes d'ordinateurs. Pour commencer, rendez-vous sur **Gestion -> Regroupement.**

Créer un groupe

Nom de groupe

Pour plusieurs groupes, séparez-les simplement par des virgules ou entrez chacun sur une nouvelle ligne.

Le nom ne peut pas contenir de caractères spéciaux <>:"*+=|?

groupe d'utilisateurs

groupe informatique

Créer un groupe

Annuler

Vous pouvez créer 3 types de groupes :

1. Groupe d'utilisateurs
2. Groupe informatique
3. Groupe d'utilisateurs et d'ordinateurs

Un **groupe d'utilisateurs uniquement** ne peut être composé que d'utilisateurs. Le regroupement d'utilisateurs est utile pour définir des autorisations d'accès pour plusieurs utilisateurs à la fois. Il est également utile pour appliquer automatiquement des autorisations d'accès à un nouvel utilisateur.

Un **groupe d'ordinateurs uniquement** ne peut être composé que d'ordinateurs. Le regroupement d'ordinateurs permet d'organiser une grande liste d'ordinateurs pour faciliter la navigation. Il peut également faciliter l'attribution des autorisations d'accès ; vous pouvez accorder à un utilisateur l'accès à un groupe entier d'ordinateurs.

Un **groupe d'utilisateurs et d'ordinateurs** est un raccourci pour le contrôle d'accès par groupe. Il peut être constitué d'utilisateurs et d'ordinateurs. Par défaut, tous les utilisateurs de ce groupe peuvent accéder à tous les ordinateurs de ce groupe.

Ajouter des utilisateurs ou des ordinateurs à un groupe

Depuis **Gestion -> Groupement**, utilisez l'icône en forme d'engrenage à droite du groupe pour affecter des utilisateurs ou des ordinateurs. Plusieurs utilisateurs ou ordinateurs peuvent être ajoutés en même temps. Vous pouvez également affecter un administrateur de groupe.

Depuis **Gestion -> Tous les ordinateurs**, utilisez l'icône d'engrenage à droite de chaque ordinateur pour affecter cet ordinateur à un groupe.

Depuis **Gestion -> Utilisateurs**, utilisez l'icône d'engrenage à droite de chaque utilisateur pour affecter l'utilisateur à un groupe. Vous pouvez également sélectionner le groupe d'un utilisateur lors de l'envoi d'une invitation.

6. Autorisations d'accès

Les autorisations d'accès déterminent les ordinateurs auxquels un utilisateur aura accès. Elles peuvent être configurées par le Propriétaire d'équipe ou les Administrateurs sous **Gestion -> Utilisateurs**.

Note :

- Les autorisations d'accès permettront à un utilisateur d'accéder de façon permanente aux ordinateurs, quelle que soit l'heure de la journée. Pour n'accorder l'accès que pour un créneau horaire particulier, voir *Section 7, Accès programmé*.

Vous pouvez définir des autorisations d'accès pour un seul utilisateur ou un groupe d'utilisateurs. Cliquez sur l'icône d'engrenage à droite d'un utilisateur ou d'un groupe d'utilisateurs et choisissez **Autorisation d'accès**.



	Rôle	Compte Splashtop	Afficher un nom	Etat	Contrôles Granulaire
<input type="checkbox"/>	Admin			Activé	

Par défaut, lorsqu'un utilisateur est invité :

- Les administrateurs ont accès à tous les ordinateurs
- Les membres n'ont accès à aucun ordinateur s'ils ne sont pas invités à faire partie d'un groupe
- Lorsqu'ils sont affectés à ou invités dans un groupe, les membres bénéficient d'un accès en fonction de l'autorisation du groupe

Autorisation d'accès utilisateur ()

Les administrateurs peuvent accorder aux utilisateurs/groupes d'utilisateurs l'accès aux ordinateurs/groupes d'ordinateurs.

- Tous les ordinateurs
- Seuls les ordinateurs de son groupe
- Uniquement des ordinateurs et des groupes d'ordinateurs spécifiques
- Pas d'ordinateurs
- Uniquement les ordinateurs basés sur les autorisations de groupe

Enregistrer

Annuler

Pour donner à un utilisateur ou à un groupe d'utilisateurs l'accès à plusieurs ordinateurs ou groupes d'ordinateurs, sélectionnez « Uniquement certains ordinateurs et groupes d'ordinateurs ».

- Uniquement des ordinateurs et des groupes d'ordinateurs spécifiques

Tous les groupes

Tout sélectionner / Tout effacer Ouvre tout / Réduire tout Afficher uniquement la sélection

4 ordinateurs sélectionnés

<input checked="" type="checkbox"/> > Site A 3	
<input type="checkbox"/> > Site B 2	
Nom de l'ordinateur ▲	
<input checked="" type="checkbox"/>	 Computer E
<input type="checkbox"/>	 Computer F

7. Accès programmé

L'accès programmé permet aux administrateurs de programmer l'accès à distance des utilisateurs, groupes et ordinateurs en fonction d'un créneau horaire. Le **Propriétaire d'équipe, les administrateurs et les administrateurs de groupe** ont accès au module de programmation.

Notes :

- L'accès programmé est accordé en plus des autorisations d'accès existantes des utilisateurs/groupe qui sont définies sous *Gestion -> Utilisateurs* ; elles ne remplacent PAS les autorisations d'accès existantes des utilisateurs/groupe.
- Pour les utilisateurs qui n'ont besoin que d'un accès à distance programmé, définissez leur autorisation d'accès sous *Gestion -> Utilisateurs* à « Aucun ordinateur ».

Configuration de l'Accès Programmé

1. Avant de créer de nouveaux programmes, allez sur **Gestion -> Paramètres** pour configurer le Fuseau horaire d'accès programmé. **Le fuseau horaire ne peut pas être modifié lorsqu'un programme est configuré**. Seul le propriétaire d'équipe a accès à ce paramètre.

Accès Programmé

(GMT-08:00) Pacific Time (US & Canada) (Modifier)

2. Allez sur **Gestion -> Accès programmé** et cliquez sur **Créer une ressource**.



Créez votre première ressource

L'accès planifié vous permet de gérer l'accès des utilisateurs au cours d'une période donnée.

[Créer une Ressource](#)

- Entrez le **Nom** et la **Description de la ressource (facultatif)**. La ressource contient l'ensemble des ordinateurs auxquels l'accès sera programmé.

Créer une Ressource

1 — 2 — 3
Général Ordinateurs Admin du groupe

Nom de la Ressource

Ordinateurs de comptabilité

La description (optionnelle)

Ressource pour ensemble d'ordinateurs utilisés par les comptables de notre entreprise.

Réglages Avancés ▾

- Cliquez sur **Paramètres avancés** si vous souhaitez activer [Pool de connexions](#) ou [Accès exclusif](#) pour cette ressource. Il s'agira alors du modèle par défaut pour les paramètres de chaque planification que vous créez.
 - Le pool de connexions permet à vos utilisateurs de se connecter à n'importe quel ordinateur disponible dans la ressource. Ceci est utile dans les cas où l'ordinateur auquel l'utilisateur se connecte n'a pas d'importance.
 - L'accès exclusif empêche un utilisateur distant d'accéder à un ordinateur s'il y a déjà un utilisateur du système d'exploitation connecté à l'ordinateur. Ceci est utile pour les scénarios où il peut y avoir des utilisateurs travaillant localement sur l'ordinateur. Vous pouvez également imposer des fonctions supplémentaires telles que l'écran vide, le verrouillage du clavier et de la souris ainsi que la déconnexion d'accès après déconnexion des sessions distantes qui suivent le programme.

Réglages Avancés ^

- Prise en charge du pool de connexions pour les horaires.
Windows Streamer v3.4.6.0 uniquement
- Prise en charge de l'accès exclusif (distant ou local) pour les comptes membres.

Définir comme paramètres par défaut

- Définissez le horaire en tant que pool de connexions.
- Empêcher le membre d'accéder à un ordinateur qui a déjà été connecté.
- Autoriser l'accès à un ordinateur avec un utilisateur connecté, s'il est inactif pendant plus de: **10 minutes** v
- Écran vide et verrouiller le clavier/la souris lors d'une session.
- Après la déconnexion normale, quittez le système d'exploitation: **Immédiatement** v
- Verrouiller l'écran avant la déconnexion automatique en cas de déconnexion involontaire: **1 minute** v

"Déconnecter l'utilisateur lors d'une déconnexion" et "Verrouiller l'écran avant la déconnexion de l'utilisateur ..." nécessite Splashtop Streamer v3.4.4.0 ou version ultérieure.

5. Sélectionnez les ordinateurs et/ou les groupes que vous souhaitez mettre à disposition dans la ressource.

Créer une Ressource

1 — 2 — 3
Général — Ordinateurs — Admin du groupe

Ordinateurs

Sélectionner des Ordinateurs

Tout sélectionner / Tout effacer Ouvre tout / Réduire tout Afficher uniquement la sélection 4 ordinateurs sélectionnés

Site A 3	
<input checked="" type="checkbox"/>	Computer E
<input type="checkbox"/>	Computer F

Site B 2	
<input type="checkbox"/>	Computer G
<input type="checkbox"/>	Computer H

6. (Facultatif) Désignez un ou plusieurs [Administrateurs de groupe](#) pour aider à gérer les programmes sur cette ressource. Les administrateurs de groupe peuvent visualiser toute ressource à laquelle ils sont affectés et peuvent également créer de nouvelles ressources et de nouveaux programmes.

Créer une Ressource



Attribuer un administrateur de groupe (optionnelle)

Sélectionnez Administrateur de groupe

7. Continuez en cliquant sur **Créer un horaire**, ou plus tard, cliquez sur le nom de la ressource pour attribuer des programmes.

La gestion / Accès Programmé

Accès Programmé

- Créer une ressource pour sélectionner un ensemble
- Les autorisations d'accès programmé sont accordées
- Les autorisations d'accès programmé ne remplacent pas

Créer une Ressource

Nom de la Ressource

Ordinateurs de comptabilité
Ressource pour ensemble d'ordinateurs utilisés par

Ajout d'une horaires pour terminer la configuration

Vous avez créé la ressource avec succès. Vous pouvez désormais créer une horaires permettant aux utilisateurs d'accéder aux ordinateurs et groupes d'ordinateurs associés.

[Ultérieurement](#) **Créer un Horaire**

8. Créez un programme pour la ressource en remplissant le **Nom**, la **Date de début** et la **Réurrence**.

Créer un Horaire

Nom du Horaire

Bilan de fin de semaine

La description (optionnelle)

Le [comptable accède à l'ordinateur](#) pour revoir les [dépenses de la semaine dernière tous les lundis](#)

Temps

Le fuseau horaire est en **GMT +00:00 (UTC)**.

2021-06-01

06:00 - 21:00

Répéter

Hebdomadaire

dim lun mar mer jeu ven sam

La répétition se termine le (optionnelle)

Choisissez la Date de Fin

Paramètres en cours de session

Forcer la déconnexion de la session à la fin du horaire.

Notifier les utilisateurs avant la fin de la session :

5 minutes

Réglages Avancés

Paramètres de connexion

Définissez le horaire en tant que pool de connexions.

Associer des Groupes D'utilisateurs (max: 250)

Veillez remplir les noms des groupes

Sélectionner Groupe

Utilisateurs Associés (max: 1000)

Veillez renseigner les adresses e-mail de vos utilisateurs

Ajouter Utilisateur

Attribuer un administrateur de groupe (optionnelle)

Sélectionnez Administrateur de groupe

- Sélectionnez des groupes d'utilisateurs et/ou des utilisateurs spécifiques pour accéder au programme.
Vous pouvez également copier/coller une liste d'adresses e-mail d'utilisateurs dans la boîte Utilisateurs.
- La sélection du menu déroulant de l'heure se fait par intervalles de 30 minutes, mais vous pouvez saisir n'importe quelle valeur à la minute près.
- Vous pouvez sélectionner plusieurs jours dans une récurrence hebdomadaire.
- Cochez la case « Forcer la déconnexion de la session à la fin du programme » si vous souhaitez que les sessions se déconnectent de force à la fin du créneau horaire.
Remarque : Cela ne déconnecte pas automatiquement le compte utilisateur du système d'exploitation de l'ordinateur.
- Cliquez sur Paramètres avancés pour gérer les paramètres Pool de connexions et Accès exclusif s'ils sont activés dans la ressource.

Gestion des ressources et programmes

Cliquez sur le menu situé à droite de chaque ressource pour afficher les options de gestion.

Nom de la Ressource	Ordinateurs	Admin du groupe
Ordinateurs de comptabilité Ressource pour ensemble d'ordinateurs utilisés par les comptables de notre ent...	Ajouter	Aucun

...

- Gérer le Horaire
- Modifier
- Supprimer

- **Gérer le programme** permet d' accéder à la vue calendrier de la ressource.
- **Modifier** permet de changer les configurations de la ressource.
- **Supprimer** permet de supprimer la ressource.

Cliquez sur un programme dans la vue calendrier pour gérer les fonctions du programme.

Ordinateurs de comptabilité

Créer un Horaire < > juin 2021 Mois ▾

lundi	vendredi	samedi	dimanche	lundi 7 juin
31 06:00 Bilan de...	4	5	6	06:00 Bilan de fin de sema... 21:00
7 06:00 Bilan de...	11	12	13	
14 06:00 Bilan de...	18	19	20	
21 06:00 Bilan de...	22	23	24	
	25	26	27	

Bilan de fin de semaine

Le comptable accède à l'ordinateur pour revoir les dépenses de la semaine dernière tous les lundis

🕒 06:00 - 21:00 7 juin 2021

⚠ Forcer la déconnexion de la session à la fin de la horaire et avertir l'utilisateur 5 minutes en avance.

Groupes 0 ▾

Utilisateurs 0 ▾

Admin du groupe
Aucun

Modifier Supprimer

⋮

- Cloner
- Pause

- **Modifier** permet de changer les configurations du programme.
- **Supprimer** permet de supprimer toutes les récurrences d'un programme.
- **Cloner** permet de créer facilement un nouveau programme avec des configurations similaires.
- **Mettre en pause/Reprendre** permet de mettre en pause ou reprendre la récurrence d'un programme. (p. ex. : vacances, maintenance)

Si un administrateur de groupe est supprimé, qu'advient-il de ses ressources/programmes ?

Si un administrateur de groupe est retiré de l'équipe ou si ses privilèges d'administrateur sont révoqués, les ressources qui lui appartiennent deviennent « inactives ».

Nom de la Ressource	Ordinateurs	Admin du groupe	
Inactif Ordinateurs de comptabilité Ressource pour ensemble d'ordinateurs utilisés par les comptables de notre ent...	Ajouter	Aucun	...

1. Pour réactiver une ressource, cliquez sur le menu à droite de la page **Ressource -> Modifier**.

Nom de la Ressource	Ordinateurs	Admin du groupe	
Inactif Ordinateurs de comptabilité Ressource pour ensemble d'ordinateurs utilisés par les comptables de notre ent...	Ajouter	Aucun	...

Gérer le Horaire

Modifier

Supprimer

2. Changez le **Statut** de la ressource : **Inactif -> Actif**.

Modifier la Ressource

État de la ressource: Inactif ?

1 — 2 — 3
Général — Ordinateurs — Admin du groupe

Nom de la Ressource

La description (optionnelle)

Statut

Inactif

Si une ressource appartient à plusieurs administrateurs de groupe, la ressource ne devient inactive que lorsque tous les administrateurs de groupe auront été supprimés.

8. Paramètres d'équipe

Allez sur **Gestion -> Paramètres** pour examiner et configurer les paramètres d'équipe. Les paramètres d'équipe contrôlent les politiques importantes pour votre équipe, telles que les capacités des fonctionnalités et l'authentification. Cette page n'est accessible que par le propriétaire d'équipe .

Aperçu des paramètres d'équipe

Paramètres

Résumé du compte
Équipe
Abonnements
Paieement et facturation
historique de paiement
Utiliser le code

Splashtop Enterprise Paramètres - 5 techniciens simultanés et 20 utilisateurs

Nom équipe	<input type="text" value=""/> s team (Modifier)
ordinateurs	16 des 1200 ordinateurs déployés (changer)
La gestion	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Activer le transfert de fichiers<input checked="" type="checkbox"/> Activer l'impression à distance<input checked="" type="checkbox"/> Activer la redirection de périphérique (configuration détaillée)<input checked="" type="checkbox"/> Activer l'entrée microphone de redirection<input checked="" type="checkbox"/> Activer le copier-coller de texte brut<input checked="" type="checkbox"/> Activer le réveil à distance<input checked="" type="checkbox"/> Activer le redémarrage à distance<input checked="" type="checkbox"/> Activer le chat (pré-session).<input checked="" type="checkbox"/> Activer l'enregistrement de session (accès sans surveillance) (configuration détaillée)<input checked="" type="checkbox"/> Activer l'enregistrement de session (accès assisté) (configuration détaillée)<input checked="" type="checkbox"/> Activer le partage de mon bureau ⓘ (accès sans surveillance)<input checked="" type="checkbox"/> Activer le partage de mon bureau ⓘ (accès assisté)<input checked="" type="checkbox"/> Activer les sessions distantes simultanées (accès sans surveillance)<input checked="" type="checkbox"/> Activer les sessions distantes simultanées (accès assisté)<input checked="" type="checkbox"/> Activer l'invite de commande à distance<input checked="" type="checkbox"/> Activer les scripts 1 à plusieurs pour <input style="width: 150px;" type="text" value="propriétaire de l'équipe uniquement"/><input checked="" type="checkbox"/> Activer le rôle d'administrateur spécifique au groupe (en savoir plus)<input checked="" type="checkbox"/> Activer l'affichage de l'utilisateur Windows ou Mac actuellement connecté<input type="checkbox"/> Autoriser les membres à accéder à l'onglet Gestion<input type="checkbox"/> Autoriser les membres à voir les groupes<input checked="" type="checkbox"/> Autoriser les utilisateurs à enregistrer les informations d'identification Windows / Mac (saisies lors du démarrage d'une session)<input checked="" type="checkbox"/> Autoriser les utilisateurs à enregistrer le code de sécurité (entré lors du démarrage d'une session)<input type="checkbox"/> Autoriser les membres à se connecter aux ordinateurs qui sont dans une session active<input type="checkbox"/> Autoriser les membres à établir des sessions simultanées<input type="checkbox"/> Autoriser les membres à déconnecter les sessions des autres<input type="checkbox"/> Autoriser les membres à redémarrer les ordinateurs et à redémarrer Streamer

Nom de l'équipe : C'est le nom que les utilisateurs verront dans leur invitation d'équipe et leurs informations de compte. Le nom de l'équipe est également affiché dans l'onglet Statut des Splashtop Streamers déployés.

Ordinateurs : Le nombre de Streamers déployés sur le total maximum.

Gestion : Ces cases permettent de contrôler les capacités des fonctionnalités, les options de visibilité et les protocoles de sécurité de l'équipe. La plupart des paramètres s'appliquent de manière globale : ils seront activés/désactivés pour tous les utilisateurs de l'équipe, quel que soit leur rôle. Certains paramètres sont basés sur les rôles, notamment :

- Permettre les sessions distantes simultanées (deux utilisateurs sur un seul ordinateur)
 - Permettre aux membres de se connecter aux ordinateurs sur une connexion active
- Permettre aux membres d'accéder à l'onglet Gestion

- Permettre aux membres de voir les groupes (uniquement les noms de groupes des ordinateurs auxquels ils ont accès)
- Permettre aux membres d'établir des sessions simultanées (connexion à plusieurs ordinateurs)
- Permettre aux membres de déconnecter les sessions d'autres membres
- Permettre le redémarrage à distance (redémarrage normal, redémarrage du streamer, redémarrage en mode sécurisé)
 - Permettre aux membres de redémarrer les ordinateurs et les streamers

Accès Programmé	(GMT+00:00) UTC (Modifier)
Notification	Configurer les e-mails de notification
Vérification en deux étapes	Gérer les appareils de confiance <input checked="" type="checkbox"/> Autoriser les utilisateurs à faire confiance aux appareils <input type="checkbox"/> Exiger des administrateurs qu'ils utilisent la vérification en deux étapes <input type="checkbox"/> Obliger les membres à utiliser la vérification en deux étapes
Authentification de l'appareil	Envoyer un lien d'authentification du périphérique de messagerie vers <input type="text" value="utilisateur seulement"/>
Authentification du navigateur	Envoyer un lien d'authentification du périphérique de messagerie vers <input type="text" value="utilisateur seulement"/>
Sécurité des terminaux	Notifier les menaces informatiques par e-mail à <input type="text" value="Aucun"/>
Délai d'expiration du navigateur	Déconnectez les utilisateurs de la console Web lorsqu'ils sont inactifs pendant <input type="text" value="Jamais"/> ⓘ
Intégration tierce	Configurer les clés API
Single Sign On	Demander une nouvelle méthode SSO (Afficher les instructions)
Jeton d'approvisionnement SCIM	(Configurer un jeton API)

Accès au programme : Définissez le fuseau horaire du module de programmation.

Indicateur de session : Configurez une [bannière persistante](#) à afficher pendant les sessions à distance pour informer les utilisateurs finaux de la session en cours sur l'ordinateur.

Notification : Configurez des notifications par e-mail pour certaines actions de l'équipe, par exemple lorsqu'un ordinateur est ajouté, lorsqu'une connexion est établie, lorsqu'un utilisateur accepte l'invitation de l'équipe, etc.

Vérification en deux étapes : Obligez les administrateurs et/ou les membres à utiliser la [Vérification en deux étapes](#) (2FA).

Authentification du dispositif/navigateur : Déterminez qui reçoit les liens d'[authentification du dispositif](#) pour les nouvelles connexions à l'application Business ou à la console Web. L'authentification par e-mail est désactivée si l'utilisateur a déjà activé la 2FA.

Intégration tierce : Si vous disposez de licences techniciens permettant d'utiliser Splashtop SOS, vous pouvez [configurer des clés API](#) pour intégrer Splashtop SOS à votre solution d'assistance ServiceNow, Zendesk, Freshservice, Freshdesk ou Jira existante.

Single Sign-On : Appliquez et gérez les méthodes d'authentification unique ici.

9. Contrôles granulaires

Avec les contrôles granulaires, vous pouvez activer ou désactiver certaines fonctionnalités pour des utilisateurs ou des groupes spécifiques.

Les contrôles granulaires sont actuellement disponibles pour :

- Transfert de fichiers
- Copier et coller
- Vérification en deux étapes
- Impression à distance
- Accès avec surveillance (licence de technicien)
- 1-to-Many (licence Technicien)

À partir de **Gestion -> Paramètres**, vous pouvez définir les **Paramètres granulaires par défaut** de ces fonctionnalités par rôle d'utilisateur. Ces paramètres par défaut sont appliqués lorsqu'un nouvel utilisateur est invité dans le groupe par défaut de l'équipe ou si le paramètre de contrôle granulaire d'un utilisateur/groupe est défini pour suivre le paramètre par défaut. Le paramètre **Configurable par l'administrateur** peut être coché si vous souhaitez également autoriser les administrateurs à vous aider à gérer les contrôles granulaires.

Paramètres granulaires par défaut	Admin	Membre	Administrateur configurable ?
Accès assisté	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transfert de fichier	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Impression à distance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Copier coller	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sous **Gestion -> Utilisateurs**, vous pouvez configurer le contrôle granulaire par utilisateur ou groupe d'utilisateurs. Pour configurer les paramètres de contrôle granulaire d'un groupe d'utilisateurs, cliquez sur l'icône de paramètres du groupe -> Contrôle granulaire.



Pour le configurer en fonction de chaque utilisateur, cliquez sur chacune des icônes de fonctionnalité pour l'activer ou la désactiver ou cliquez sur l'icône de paramètres de l'utilisateur -> Contrôle granulaire.

Contrôles Granulaires	
	Contrôle granulaire Attribuer un groupe d'util

Contrôle granulaire	
	État
Accès assisté	Actif ▼
Transfert de fichier	Inactif ▼
Impression à distance	Par défaut ▼
Copier coller	Actif ▼

- **Activé** : activer cette fonctionnalité pour l'utilisateur.
- **Désactivé** : désactiver cette fonctionnalité pour l'utilisateur.
- **Suivre le groupe** : Appliquer le paramètre du groupe d'utilisateurs à l'utilisateur.
- **Par défaut** : Appliquer le paramètre par défaut de l'équipe en fonction du rôle de l'utilisateur selon les paramètres granulaires par défaut de l'équipe.

10. Gestion des ordinateurs à distance (techniciens)

Les **licences de technicien** comprennent des fonctionnalités permettant de gérer les ordinateurs à distance avec la possibilité de consulter les journaux d'événements Windows, l'inventaire système/matériel/logiciel, la sécurité des terminaux et de gérer les mises à jour Windows et les alertes configurables. Vous pouvez également envoyer des commandes à l'invite de commande d'un ordinateur distant sans surveillance en arrière-plan. Toutes les fonctionnalités décrites sont disponibles pour le **propriétaire d'équipe et les administrateurs** sauf indication contraire.

Journaux des événements Windows

Affichez les journaux d'événements Windows d'un ordinateur en ligne dans la console Web Splashtop. Vous pouvez filtrer par niveau d'événement, type d'événement, date et ID de l'événement.

Afficher les journaux des événements:

Niveau d'événement: Critical Error Warning Information

Type d'événement: System Application Security Setup

De 2021-05-28 00 : 00 à 2021-05-28 23 : 59

Inclure des informations détaillées: Oui Non

Filtre d'ID d'événement: ⓘ

Récupérer

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Inventaire informatique – Système, matériel, logiciel

Visualisez et comparez des instantanés de l'inventaire système, matériel ou logiciel d'un ordinateur. Cette vue est disponible par ordinateur individuel. Vous pouvez également exporter l'inventaire de tous les ordinateurs en cliquant sur l'option **Exporter** en bas de la page **Gestion -> Tous les ordinateurs**, ou tout consulter dans **Gestion -> Inventaire**.

Affichez l'inventaire du système de test:

Afficher les instantanés de 2021-05-28

Comparer des instantanés 2021-05-27 et 2021-05-28

Afficher le journal des modifications de à

L'instantané du 2021-05-28 a été mis à jour le 2021-05-28 03:19:06 -0700. (Actualisez l'inventaire du système d'aujourd'hui)

Appliquer

Logiciel

	2021-05-27	2021-05-28
Software 1	Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated Version: 21.001.20155	Name: Adobe Acrobat Reader DC Vendor: Adobe Systems Incorporated Version: 21.001.20155

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Sécurité des points terminaux

Consultez l'état de sécurité des terminaux pour les ordinateurs Windows sur **Gestion -> Sécurité des terminaux** pour vous assurer que toutes les machines sont protégées. Vous pouvez également acheter une licence supplémentaire de Bitdefender afin de pouvoir installer et analyser directement depuis la console web Splashtop. **Le tableau de bord Endpoint Security est disponible pour le propriétaire de l'équipe, les administrateurs et les administrateurs de groupe.**

	Actions ▾	Acheter Bitdefender	Tous les ordinateurs ▾	[redacted]'s Computers ▾			
Statut	Nom de l'ordinateur ▾	Groupe	Logiciel	protection	Heure du dernier scan	Des menaces ¹	Détails
<input type="checkbox"/>	test	[redacted]'s Computers	Bitdefender Endpoint Security Tools Antimalware	Activé	2021-05-22 07:00:00	54	
Tâche d'analyse: N/A							

[Reconnaitre toutes les menaces](#)

	Nom de la menace	Horodatage détecté	Nom d'objet	action	Reconnu
	Gen:Illusion.ML.Skyline.B.2010101	2021-02-13 10:31:10 -0800	C:[redacted]	REMOVED	Reconnaitre
	Gen:Illusion.ML.Skyline.B.2010101	2021-02-12 14:00:00	C:[redacted]		Reconnaitre

[Consultez cet article pour obtenir plus de détails et d'instructions sur Bitdefender.](#)

Mises à jour Windows

Vérifiez l'état des mises à jour Windows d'un ordinateur sur **Gestion -> Mises à jour Windows**. Cliquez sur **Détails** pour vérifier, afficher et pousser les mises à jour disponibles immédiatement ou à une heure programmée pour un ordinateur spécifique.

	Actions ▾	Tous les ordinateurs ▾	[redacted]'s Computers ▾					
État de mise à jour	Nom de l'ordinateur ▾	Groupe	OS	Important	Optionnel	Politique de mise à jour	Heure de la dernière mise à jour	Détails
<input type="checkbox"/>	test	[redacted]'s Computers	Microsoft Windows 10 Pro 64-bit (10.0.18363)	0	2	Installer des mises à jour automatiquement	2021-05-28 20:24:36 UTC	
<input type="checkbox"/>	laptop test	[redacted]'s Computers	Microsoft Windows 10 Home 64-bit (10.0.18363)	1	3	Installer des mises à jour automatiquement	2021-05-26 06:50:54 UTC	

Mises à jour disponibles: 0 important, 2 facultatif [Vérifier les mises à jour](#) Inclure des mises à jour pour d'autres produits Microsoft
 (Dernière vérification des mises à jour: 2021-05-28 10:05:11 +0000)

<input type="checkbox"/>	Code	Important	Redémarrer	Taille	Mettre à jour
<input type="checkbox"/>	4589211	No	Yes	3 MB	2021-01 Update for Windows 10 Version 1909 for x64-based Systems (KB4589211) - Install this update to resolve issues

Actions 1-to-Many et calendriers

Créez une action 1-to-Many qui vous permet d'exécuter ou de planifier immédiatement une tâche sur plusieurs ordinateurs ou groupes d'ordinateurs. Configurez un redémarrage du système, une mise à jour Windows ou déployez discrètement un fichier .EXE, .MSI, .PKG et plus encore. Vous pouvez réaliser ces actions en accédant à **Gestion -> Actions 1-to-Many** ou **Programmes 1-to-Many**.

Les actions qui doivent être exécutées immédiatement ne peuvent l'être que sur des ordinateurs en ligne. Si un ordinateur est hors ligne lorsqu'une action programmée est tentée, il n'y a actuellement aucun mécanisme permettant de renouveler la tentative.

1-to-Many est uniquement disponible pour le propriétaire de l'équipe, ou le propriétaire de l'équipe et les administrateurs, selon l'option sélectionnée dans **Gestion -> Paramètres**.

Activer les scripts 1 à plusieurs pour propriétaire de l'équipe uniquement

- propriétaire de l'équipe uniquement
- propriétaire de l'équipe et tous les administrateurs

Par ailleurs, l'autorisation peut également être configurée dans Contrôles granulaires.

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Alertes configurables

Configurez des alertes configurables sous **Gestion -> Profils d'alerte** pour être averti lorsque certaines actions se produisent. Il peut s'agir d'un logiciel installé/désinstallé, de l'utilisation du processeur/disque, du passage en ligne/hors ligne l'ordinateur, etc.

Nom du profil d'alerte (Activé) ➔ Ajouter une ou plusieurs

Utilisation du processeur (Activé)

Nom: Type: Utilisation du processeur

Utilisez cette alerte pour surveiller l'utilisation du processeur. Une alerte est déclenchée lorsque l'utilisation est supérieure ou égale au s

Alerte lorsque l'utilisation moyenne du processeur est supérieure ou égale à % pendant

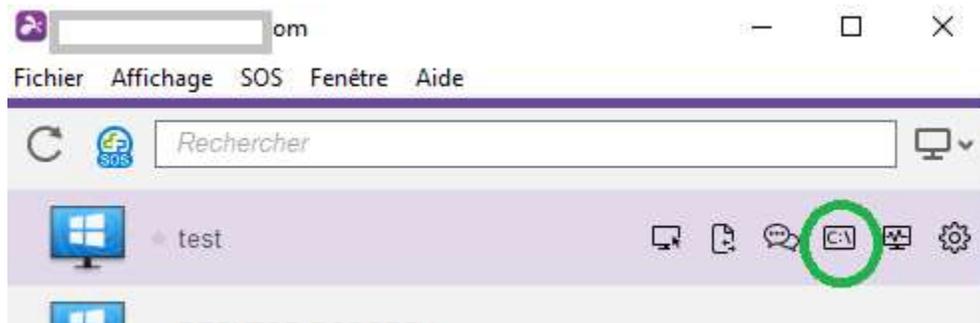
Informez également par e-mail pour alerte reconnaissance récupération Joignez également le lien de connexion d'alerte

- Utilisation du processeur
- Utilisation de la mémoire
- Espace disque
- Ordinateur en ligne
- Ordinateur hors ligne
- Logiciels installés
- Logiciel désinstallé
- Windows Update
- Mises à jour disponibles
- Journal des événements Windows

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Commande à distance

Depuis l'application [Business](#), cliquez sur l'icône de commande à distance d'un ordinateur pour envoyer des commandes de ligne de commande ou de terminal à un ordinateur Windows ou Mac distant en arrière-plan.

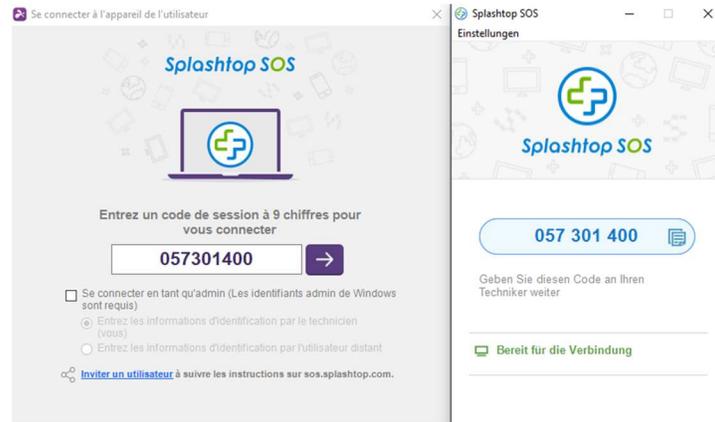


Cette fonctionnalité est disponible pour tous les utilisateurs de l'équipe si elle est activée, et nécessite que l'utilisateur saisisse les identifiants d'administration de l'ordinateur distant pour y accéder.

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

11. Accès avec surveillance - SOS (techniciens)

Les **licences de technicien** permettent de profiter d'un accès sous surveillance avec Splashtop SOS. Utilisez Splashtop SOS pour accéder aux appareils Windows, Mac, iOS, Android et Chromebook avec un code de session à 9 chiffres.



Pour vous connecter, entrez le code de session à 9 chiffres généré par l'utilisateur final qui exécute l'application Splashtop SOS. [Voir le tutoriel ici.](#)

Fonctionnalités supplémentaires :

- [Connexion avec droits d'administration](#)
- [Changement d'utilisateur du système d'exploitation](#)
- [Redémarrage et reconnexion](#)
- [SOS en marque blanche](#)
- [Intégrations avec ITSM/service d'assistance](#) (ServiceNow, Freshservice, Freshdesk, Zendesk, Jira et plus encore à venir)

Paramètres granulaires

Configurez qui peut utiliser l'accès sous surveillance avec des paramètres granulaires. Le propriétaire de l'équipe peut configurer l'autorisation d'accès sous surveillance par défaut par rôle d'utilisateur sous **Paramètres de gestion** ->. Cela détermine l'autorisation d'accès sous surveillance par défaut d'un utilisateur lorsqu'il est invité dans l'équipe.

Paramètres granulaires par défaut	Admin	Membre	Administrateur configurable ?
Accès assisté	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Sous **Gestion** -> **Utilisateurs**, vous pouvez également configurer l'autorisation d'accès sous surveillance par utilisateur individuel ou groupe d'utilisateurs.

IT Team	Rôle	Compte Splashtop	Afficher un nom	Etat	Contrôles Granulaire	Contrôle granulaire droit d'accès
<input type="checkbox"/>	Admin			Activé	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

12. Personnalisation de SOS (techniciens)

Le [marquage personnalisé](#) est disponible pour l'application Splashtop SOS. Pour créer une application personnalisée, accédez à **Gestion -> Personnalisation de SOS -> Créer une application SOS**.

Personnalisation SOS

Personnalisez l'apparence et les paramètres de l'application SOS.

[+ Créer une application SOS](#)

Nom	Date de Création		
Test	10/06/2021, 16:39:50	Partager	...
Test 2	15/12/2021, 18:16:12	Partager	...
...s Test Package	24/03/2022, 00:49:38	Partager	...

Personnalisez différentes parties telles que le nom de l'application, les couleurs et les descriptions. Vous pouvez également créer une clause de non-responsabilité et configurer des paramètres supplémentaires tels que l'audio et le proxy.

Thème

Thème SOS

Thème Service Desk

Icône (Windows uniquement, taille d'image maximale 2 Mo, format : ICO)

Télécharger

Légende (max 20 caractères)

Splashtop SOS

Bannière (Taille de l'image 320 x 160, max 2 MB, format : JPG/PNG/GIF)

Télécharger

Couleur d'arrière-plan



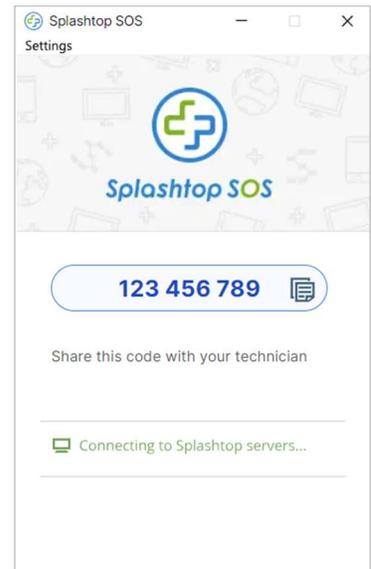
Section à 9 chiffres

123 456 789

Texte d'instruction (max 80 caractères)

Share this code with your technician

Couleur du texte d'instruction



13. Service Desk (techniciens)

[Service Desk](#) fournit une interface permettant aux techniciens de gérer une file d'attente de sessions sous surveillance et d'améliorer le flux de travail de leur équipe. Au lieu d'attendre que l'utilisateur final fournisse le code SOS à 9 chiffres, les techniciens peuvent envoyer un lien d'application personnalisé et les ajouter à une file d'attente. **Cette fonctionnalité nécessite une licence de technicien.**

Pour accéder à Service Desk, cliquez sur Service Desk dans my.splashtop.com ou sur l'icône dans l'application Splashtop Business.

The screenshot shows the Splashtop Service Desk interface. The top navigation bar includes 'Computers', 'Devices', 'Logs', 'Management', and 'Service Desk' (circled in green). The main content area is titled 'Service Desk / Company ABC' and features a 'New Session' button and a table of sessions. The table has columns for Name, Status, and Time. Below this, a secondary window shows the 'SOS' menu with the 'SOS' icon circled in green. The main content area also includes a sidebar with 'Home', 'Channels', 'Private', 'Company ABC', and 'DevOps'.

Name	Status	Time
John	Waiting	2022-04-06 05:16:28
Steven	Active	2022-03-25 17:59:16
Kai	Active	2022-04-05 18:35:16

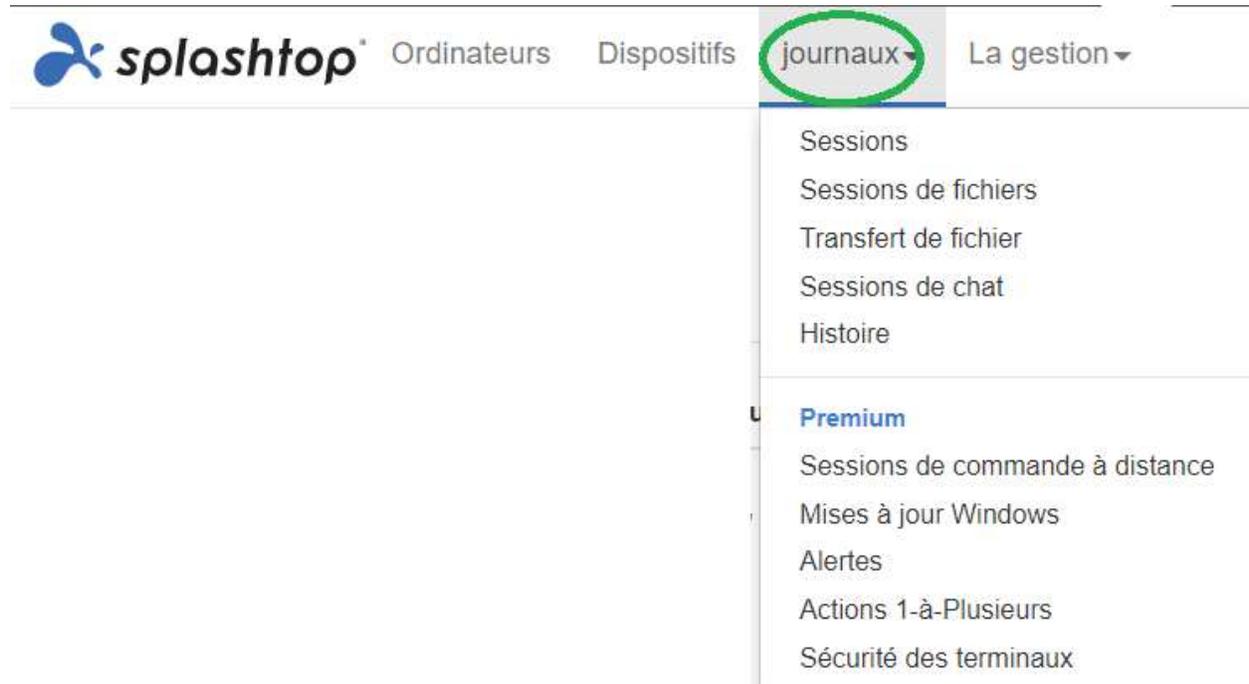
Name	Status	Time	Technician	Device
Kai	Active	2022-04-05 11:35:16	(You)	M
Steven	Active	2022-03-25 10:59:16	(You)	D
John	Waiting	2022-04-05 22:16:28	(You)	

Créez des canaux dans la console Service Desk et affectez des techniciens. Les techniciens peuvent créer des sessions d'assistance pour les clients via un lien d'invitation ou un code à 6 chiffres, ou fournir une application [SOS Call](#) que les clients peuvent lancer lorsqu'ils ont besoin d'assistance. Une fois qu'une session de support est créée, les techniciens peuvent réaffecter, transférer ou inviter d'autres techniciens dans le cadre de la session.

14. LOGS

Splashtop tient des registres pour l'auto-vérification. Le propriétaire de l'équipe et les administrateurs peuvent consulter les journaux de tous les membres de l'équipe. Les membres ne verront que leurs propres journaux.

Pour consulter les journaux, allez sur my.splashtop.com -> **Logs**.



Les journaux incluent les 7, 30 ou 60 derniers jours. Si votre service comprend à la fois un accès sans surveillance et un accès avec surveillance, vous pouvez choisir lequel vous souhaitez consulter. Faites défiler la page vers le bas jusqu'à **Exporter au format CSV** pour télécharger jusqu'à un an de journaux passés.

	Accès sans surveillance ▾	Les 7 derniers jours ▾	<input type="text"/>							
État	Heure de début	Heure de fin	Durée	Ordinateurs	Propriétaire de l'ordinateur	Connecté par	Périphérique connecté	Type	Fichier	Matière / Remarque

[Voir cet article pour obtenir un aperçu des journaux.](#)

15. Fonctionnalités supplémentaires

Ces fonctionnalités avancées supplémentaires sont disponibles avec Splashtop Enterprise.
[Contactez Splashtop Sales](#) pour plus d'informations.

Restriction IP

Limitez l'accès à la console Web <https://my.splashtop.com> ou à l'application Splashtop Business en fonction de l'adresse IP.

Business App IP/liste blanche des réseaux

Seules les demandes d'accès à votre ordinateur à partir de la liste d'adresses/réseaux suivante seront activées.

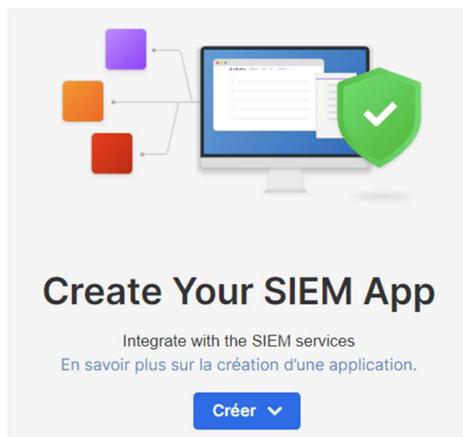
par ex. 168.168.168.168, 168.168.168.0/24



[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Création de journaux SIEM

Exportez les journaux de session et d'historique Splashtop vers un logiciel de gestion des informations et des événements de sécurité (SIEM) pour une analyse plus approfondie.

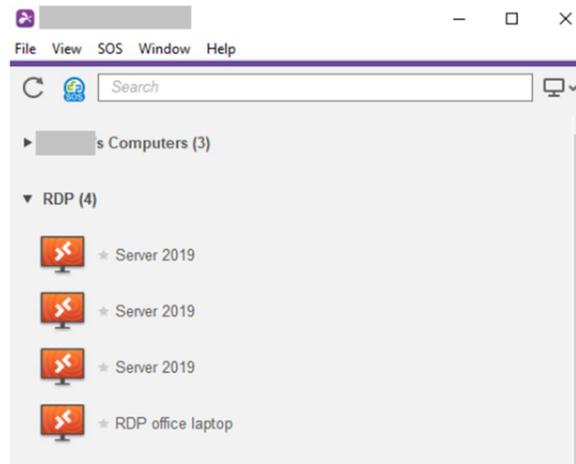


The banner features a central computer monitor displaying a document. To the left, three colored squares (purple, orange, red) are connected to the monitor by lines. To the right, a green shield with a white checkmark is positioned. Below the monitor, the text reads: 'Create Your SIEM App', 'Integrate with the SIEM services', and 'En savoir plus sur la création d'une application.' At the bottom center is a blue button with the text 'Créer' and a downward arrow.

[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Splashtop Connector

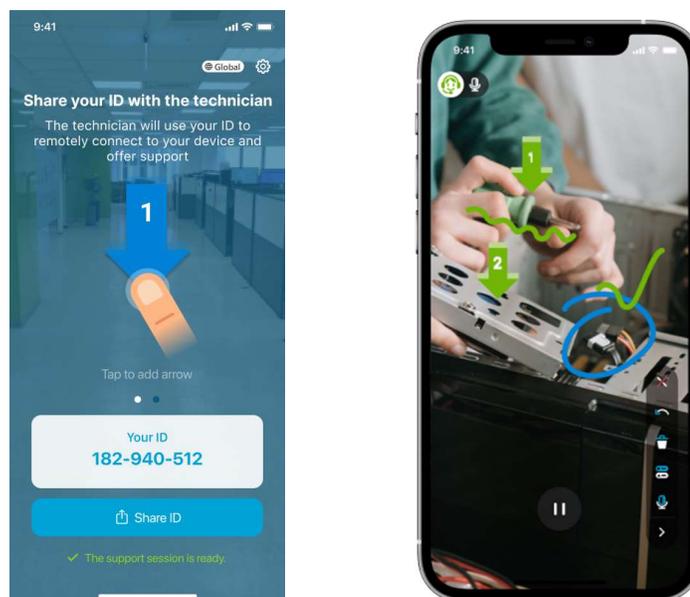
Créez des ponts sécurisés entre les connexions RDP et les ordinateurs et serveurs Windows via Splashtop sans avoir à utiliser de VPN ou à installer de logiciel sur chaque ordinateur.



[Consultez cet article pour obtenir plus de détails et d'instructions.](#)

Splashtop AR

Connectez-vous à des sites éloignés et résolvez les problèmes en direct grâce au partage de caméra et aux annotations en réalité augmentée.



[Consultez cet article pour obtenir plus de détails et d'instructions.](#)