

# Configuration d'un tunnel SSH d'assistance technique à la demande pour les appliances virtuelles Umbrella

## Table des matières

---

[Introduction](#)

[Tunnel SSH d'assistance technique à la demande](#)

[Conditions préalables](#)

[Activation du tunnel](#)

[Activation du tunnel sur les appareils virtuels hébergés sur VMware et Hyper-V](#)

[Activation du tunnel sur les appareils virtuels hébergés sur d'autres plates-formes](#)

[Obtention de vos informations d'identification à partager avec le support](#)

[Désactivation/réactivation du tunnel](#)

[États du tunnel](#)

[connected](#)

[Désactivé](#)

[Connexion](#)

[Expiration du délai](#)

[Persistance du tunnel](#)

---

## Introduction

Ce document décrit la configuration d'un tunnel SSH d'assistance technique à la demande pour les appliances virtuelles Umbrella.

## Tunnel SSH d'assistance technique à la demande

Un ingénieur de support peut demander un accès à distance à votre appliance virtuelle (VA) afin de diagnostiquer un dossier de support et éventuellement de revoir ou de mettre à jour les paramètres afin d'améliorer la disponibilité VA. Pour qu'un ingénieur de support Umbrella puisse accéder à une VA Umbrella sur site, vous devez suivre ces instructions.



Remarque : Ces informations ne s'appliquent qu'à VA avec la version 2.1.0 ou ultérieure.

---

## Conditions préalables

- Toutes les conditions requises pour la configuration d'une appliance virtuelle sur VMWare ou Hyper-V de la documentation de configuration doivent être remplies.
- Tout pare-feu doit être configuré pour autoriser les connexions sortantes vers `s.tunnels.ironport.com`.
- L'appliance virtuelle tente de se connecter successivement sur les ports TCP 22, 25, 53, 80, 443 ou 476.

Pour tester la connectivité, vous pouvez établir une connexion Telnet avec le tunnel de support :

```
telnet s.tunnels.ironport.com 25
```

```
Tentative 63.251.108.107...
```

```
Connecté à s.tunnels.ironport.com.
```

Le caractère d'échappement est '^]'.  
SSH-2.0-OpenSSH\_6.2 CiscoTunnels1

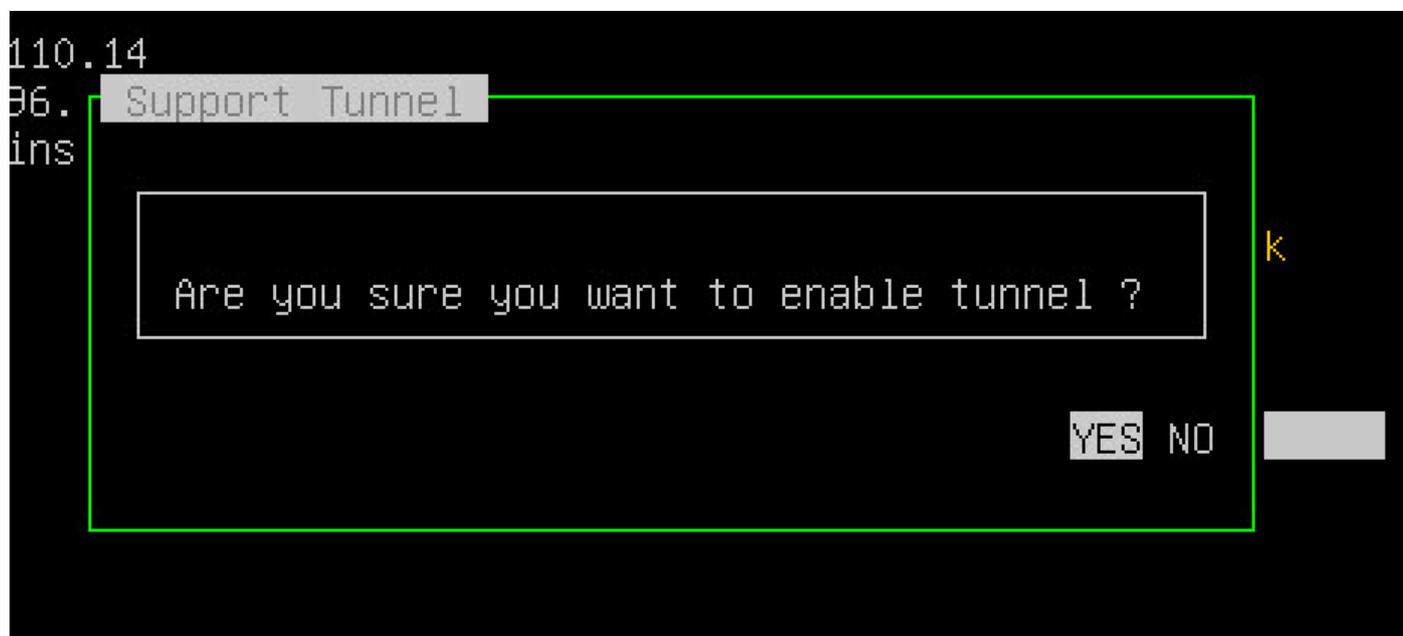
## Activation du tunnel

Le tunnel SSH se connecte à s.tunnels.ironport.com. La durée de la connexion est configurable, avec une valeur par défaut de 72 heures.

### Activation du tunnel sur les appareils virtuels hébergés sur VMware et Hyper-V

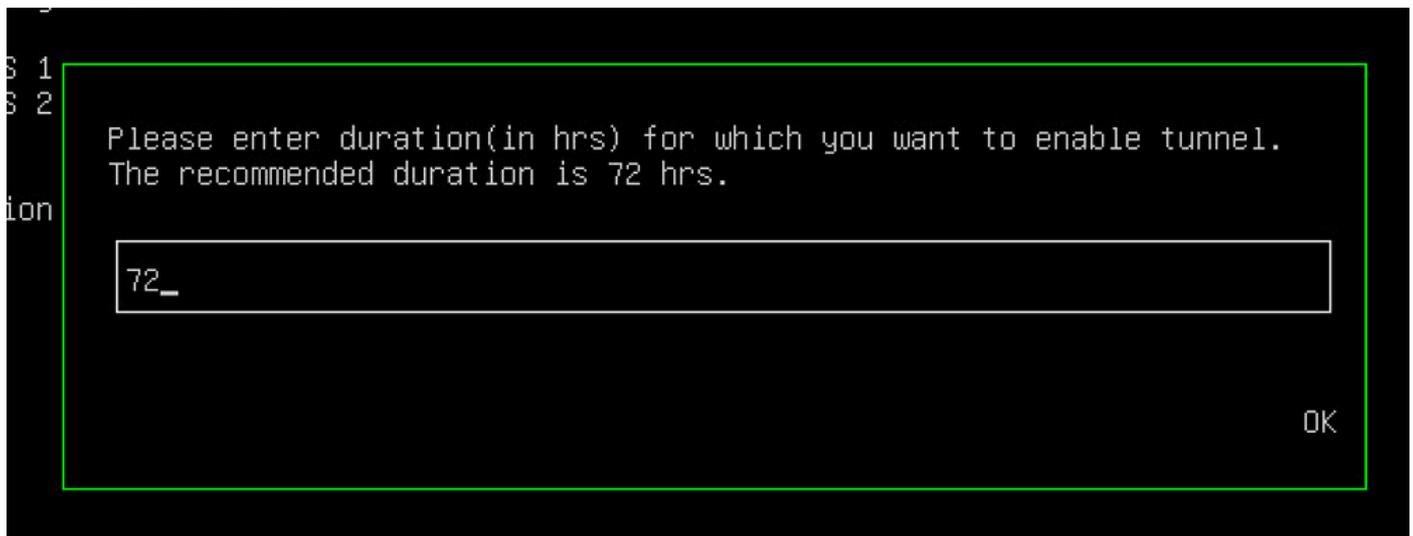
Les tunnels peuvent être activés à partir de la console de VA à l'aide de la commande de clavier "CTRL+T".

Sélectionnez Yes lorsque vous y êtes invité :



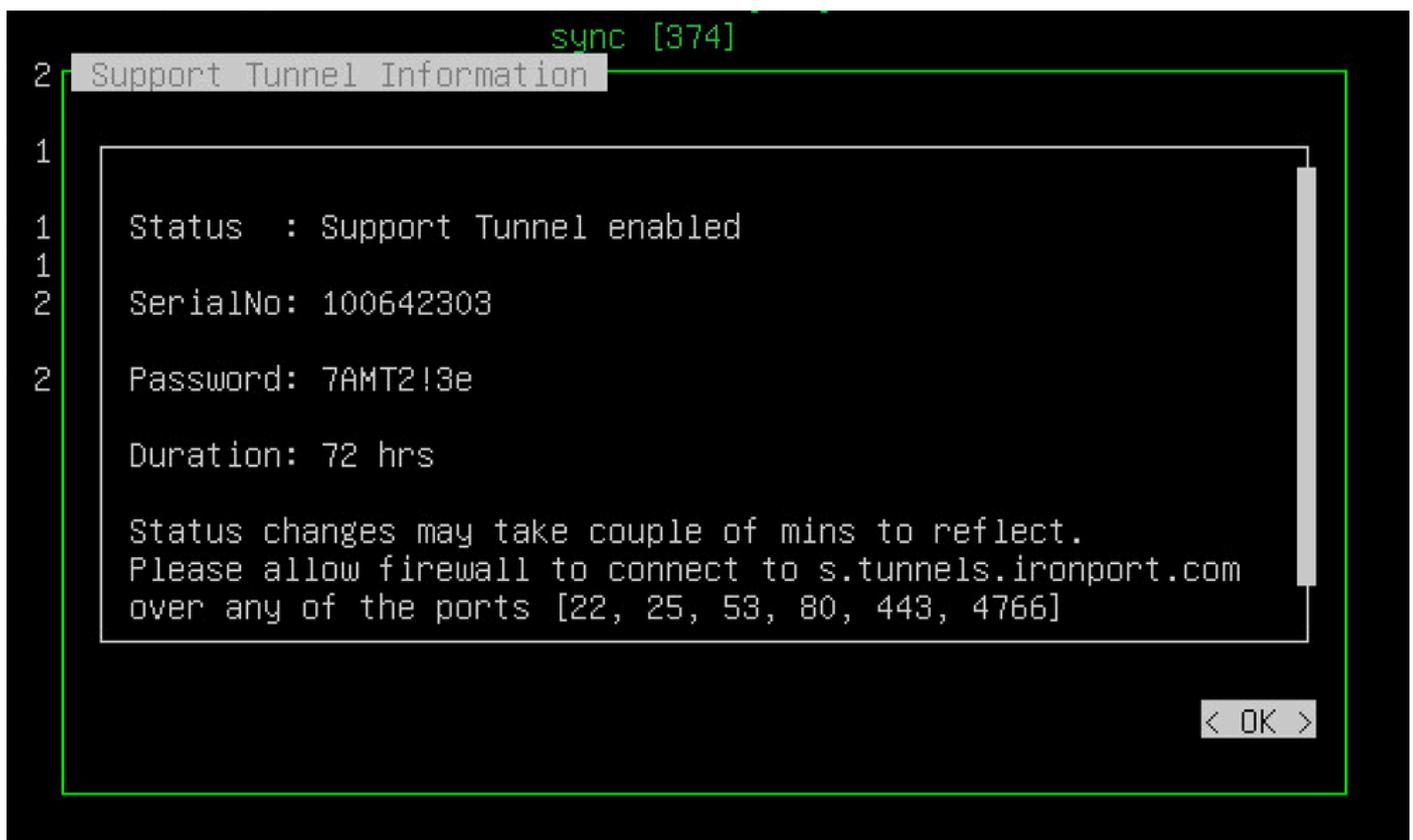
115013855903

Tout d'abord, vous êtes invité à définir la durée de la session de tunnel :



115013856003

Sélectionnez OK et une fenêtre s'affiche indiquant le numéro de série et le mot de passe du tunnel de support. Ces informations doivent être transmises au technicien de support. Après avoir sélectionné OK, l'AV tente d'établir une connexion au serveur de tunnel de support :



115013853243

Cliquez sur OK pour fermer la fenêtre. Vérifiez que la console VA affiche « Remote Support Tunnel: Connecté ».

## Connectivity

```
This DNS Server: DNS ok  
Local DNS Servers: All DNS ok  
Umbrella DNS Servers: All DNS ok  
AD Connectors: Active  
Remote Support Tunnel: Connected  
Umbrella Cloud: SSL ok  
Updates: SSL GET ok
```

360000820923

### Activation du tunnel sur les appareils virtuels hébergés sur d'autres plates-formes

Connectez-vous à l'appliance virtuelle sur SSH et utilisez la commande config comme ci-dessous :

- Pour activer le tunnel de support, entrez `config tunnel enable <duration in hours>`.
- Pour désactiver le tunnel de support, entrez `config tunnel disable`.
- Pour vérifier l'état du tunnel de support, entrez `config tunnel status`.
- Pour afficher ces options, entrez `config tunnel help`.

### Obtention de vos informations d'identification à partager avec le support

Le numéro de série et le mot de passe affichés dans la console de l'AV ou lors de l'utilisation de la commande `config tunnel status` doivent être donnés au technicien de support.



Remarque : Le mot de passe que vous récupérez et partagez avec le support ne peut pas être directement utilisé pour accéder à l'appliance virtuelle. Pour des raisons de sécurité, le mot de passe réel est cryptographiquement dérivé du mot de passe que vous voyez. Pour obtenir le numéro de série et le mot de passe à partir de la console VA, prenez une capture d'écran après avoir activé le tunnel avec Ctl+T. Assurez-vous que la capture d'écran est lisible par les utilisateurs.

---

## Désactivation/réactivation du tunnel

Le tunnel reste établi par défaut pendant 72 heures, mais vous avez la possibilité d'étendre la durée du tunnel en utilisant l'option Re-enable.

Sur VMware et Hyper-V, le tunnel peut être désactivé ou réactivé à tout moment à l'aide de la commande CTRL-T :

1

Support Tunnel

14

1

Status : Support Tunnel enabled

SerialNo: 100933673

Password: 6zGQ%c3K

S ok  
ok

ted

DISABLE RE-ENABLE OK



Remarque : L'état du tunnel peut prendre jusqu'à une minute pour passer de Connecté à Désactivé, à la fois dans l'interface utilisateur et dans le back-end, car le tunnel est arrêté en douceur au lieu d'être arrêté.

---

Sur d'autres plates-formes, vous pouvez utiliser cette commande :

- `config tunnel reenable <durée en heures>`

Si vous essayez de réactiver le tunnel immédiatement après l'avoir désactivé, cela peut entraîner une condition impaire et un message d'erreur car le tunnel n'est pas complètement désactivé à ce stade.

La réactivation du tunnel ne modifie pas le mot de passe de la session de tunnel existante de l'appliance virtuelle. Par défaut, la sélection de l'option Re-enable ajoute 72 heures de durée de tunnel à partir de l'heure actuelle.

## États du tunnel

## connected

L'état passe de Disabled à Connected dès que vous activez le tunnel. Si la connexion réussit, notez que l'état reste en mode de connexion pendant environ une minute lorsque l'appliance virtuelle tente d'établir son tunnel avec le serveur.

## Désactivé

Si vous n'avez pas explicitement activé le tunnel, l'état Disabled s'affiche. Notez qu'après avoir explicitement désactivé le tunnel, il faut environ une minute pour que l'état du tunnel passe de Connecté à Désactivé.

## Connexion

Dans l'état de connexion, l'appliance virtuelle tente d'établir le tunnel (en essayant les ports 22, 25, 53, 80, 443 et 476 de manière séquentielle) avec un délai de 5 minutes entre chaque tentative. L'appliance virtuelle reste dans cet état jusqu'à ce qu'une connexion soit établie ou que 30 minutes se soient écoulées sans qu'aucune connexion n'ait été établie.

La connexion peut échouer en raison de problèmes réseau (par exemple, des ports bloqués).

## Expiration du délai

Si l'appliance virtuelle ne parvient pas à établir une connexion avec le serveur distant, l'état passe à Délai d'attente dépassé. Le délai d'attente se produit environ 30 minutes après que l'appliance virtuelle a tenté d'établir un tunnel avec le serveur distant.

## Persistance du tunnel

Une fois qu'un tunnel de prise en charge est activé, l'appliance virtuelle respecte la valeur de durée entrée, même si l'appliance virtuelle est redémarrée ou mise à niveau. Aucune action supplémentaire n'est requise de votre part. Si l'appliance virtuelle redémarre, ou met à niveau, et que le temps reste dans la durée spécifiée, l'appliance virtuelle tente de se reconnecter automatiquement au serveur de tunnel SSH.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.