

# Récupération de mot de passe dans Cisco Guard et Traffic Anomaly Detector

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Conventions](#)

[Procédure pas à pas](#)

[Informations connexes](#)

## Introduction

Ce document décrit la procédure pour récupérer le mot de passe de l'**utilisateur de base** dans une protection de Cisco ou une appliance de réduction de Distributed Denial of Service de Traffic Anomaly Detector de Cisco (DDoS). Ce mot de passe est utilisé pour contrôler l'accès de **racine** à un système de protection de Cisco ou de Traffic Anomaly Detector de Cisco. **Le mot de passe root** est chiffré et peut seulement être remplacé par un nouveau mot de passe suivant la procédure ci-dessous.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

## Procédure pas à pas

Procédez comme suit :

1. Reliez un clavier et un moniteur à la protection de Cisco ou au Traffic Anomaly Detector de Cisco (cette procédure ne peut pas être exécutée par une interface série ou une connexion réseau.)
2. **Réinitialisation de** procédure de connexion et de type.
3. Tandis que la case met sous tension, maintenez la touche Shift appuyée sur. Ceci vous obtiendra un « démarrage de Lilo : » demande.

4. **ONGLET de** presse pour voir des images disponibles.**Note:** 3.0.8 a une image de « **Cisco** », alors que des images plus anciennes ont « **Riverhead** ».
5. Tapez **Cisco 1** pour obtenir une image de seul utilisateur chargée (ou **Riverhead 1** dans des systèmes plus anciens). Ceci démarrera le système en mode de seul utilisateur.
6. Pendant le processus de démarrage vous serez demandé un mot de passe. Écrivez le **dud&ndud de** mot de passe fixe. Ceci te donnera un shell de **racine**.
7. Maintenant vous pouvez exécuter la commande de **passwd** de changer le mot de passe de la **racine**. Vous serez invité à confirmer le mot de passe que vous avez choisi, par exemple :

```
[root@DETECTOR root]# passwd
Changing password for user root.
New password: <new password typed in here>
Retype new password: <new password typed in here>
passwd: all authentication tokens updated successfully.
```

8. Après que vous ayez changé le mot de passe, exécutez la commande de **réinitialisation** de redémarrer le système. N'interrompez pas le processus de démarrage de sorte que le système entre son mode de fonctionnement normal.

## [Informations connexes](#)

- [Dispositifs de réduction des risques Cisco Guard DDoS](#)
- [Cisco Traffic Anomaly Detectors](#)
- [Support technique - Cisco Systems](#)