

# Configurer un routeur Cisco pour l'authentification de numérotation à l'aide de TACACS+

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurations](#)

[Installation de Microsoft Windows](#)

[Microsoft Windows a installé pour les utilisateurs 1 et 2](#)

[Instructions pas à pas](#)

[Microsoft Windows a installé pour l'utilisateur 3](#)

[Vérifiez](#)

[Dépannez](#)

[Routeur](#)

[Serveur](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit comment configurer un routeur de Cisco pour l'authentification de cadran avec le TACACS+ qui fonctionne sur l'UNIX. TACACS+ n'offre pas autant de caractéristiques en tant que le [Cisco Secure ACS](#) disponible dans le commerce [pour Windows](#) ou [Cisco Secure ACS pour l'UNIX](#).

Le logiciel TACACS+ précédemment fourni par Cisco Systems a été discontinué et n'est plus pris en charge par Cisco Systems.

Aujourd'hui, vous pouvez trouver beaucoup de versions gratuites de TACACS+ quand vous recherchez « logiciel gratuit TACACS+ » sur votre moteur de recherche préféré sur Internet. Cisco ne recommande spécifiquement aucune implémentation particulière de logiciel gratuit TACACS+.

Le Cisco Secure Access Control Server (ACS) est disponible pour l'achat par des ventes de Cisco et des canaux réguliers de distribution dans le monde entier. Le Cisco Secure ACS pour des Windows inclut tous les composants nécessaires requis pour une installation indépendante sur une station de travail de Microsoft Windows. Le moteur de solution de Cisco Secure ACS est expédié avec une licence logicielle préinstallée de Cisco Secure ACS. Référez-vous au [bulletin de produit du Cisco Secure ACS 4.0](#) pour des nombres de produit. Visitez la [page d'accueil de](#)

[commande Cisco](#) (clients [enregistrés](#) seulement) pour passer une commande.

**Note:** Vous avez besoin d'un compte CCO avec un contrat de service associé d'obtenir la version test de 90-jour pour le [Cisco Secure ACS pour Windows](#) (clients [enregistrés](#) seulement).

La configuration du routeur dans ce document a été développée sur un routeur qui exécute la version software 11.3.3 de Cisco IOS®. Les versions du logiciel Cisco IOS 12.0.5.T et l'utilisation postérieure **groupent tacacs+** au lieu de **tacacs+**. Les déclarations telles que **l'enable de l'aaa authentication login default tacacs+** apparaissent comme **enable du groupe tacacs+ d'aaa authentication login default**.

Vous pouvez télécharger le guide de logiciel gratuit et d'utilisateur TACACS+ par Anonymous FTP à <ftp-eng.cisco.com> dans le répertoire de [/pub/tacacs](#).

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

### Conventions

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

## Configurations

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Note:** Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[outil de recherche de commande](#) (clients [enregistrés](#) uniquement).

Ce document utilise les configurations suivantes :

- [Configuration du routeur](#)
- [Fichier de configuration TACACS+ sur le serveur gratuit](#)

### **Configuration du routeur**

```
!  
aaa new-model  
aaa authentication login default tacacs+ enable  
aaa authentication ppp default if-needed tacacs+  
aaa authorization exec default tacacs+ if-authenticated  
aaa authorization commands 1 default tacacs+ if-
```

```

authenticated
aaa authorization commands 15 default tacacs+ if-
authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&hl&r2&c1&d2&ble0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
!--- Challenge Handshake Authentication Protocol !---
(CHAP/PPP) authentication user. interface Async1 ip
unnumbered Ethernet0 encapsulation ppp async mode
dedicated peer default ip address pool async no cdp
enable ppp authentication chap ! !--- Password
Authentication Protocol (PAP/PPP) authentication user.
interface Async2 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool
async no cdp enable ppp authentication pap ! !---
Authentication user with autocommand PPP. interface
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end

```

### Fichier de configuration TACACS+ sur le serveur gratuit

```

!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }

```

## [Installation de Microsoft Windows](#)

### [Microsoft Windows a installé pour les utilisateurs 1 et 2](#)

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce

document.

## Instructions pas à pas

Procédez comme suit :

**Note:** La configuration de PC peut varier légèrement basé sur la version du système d'exploitation que vous utilisez.

1. Sélectionnez le **début** > le **Programs** > **Accessories** > **Dial Up Networking** pour ouvrir la fenêtre commutée de réseau.
2. Choisissez **établissent le nouveau rapport** à partir du menu de connexions, et écrivent un nom pour votre connexion.
3. Écrivez vos informations de modem-particularité et cliquez sur Configurer.
4. À la page du Général Properties sélectionnez la vitesse la plus élevée de votre modem, mais ne cochez pas le **seul se connectent à cette** case de **vitesse**....
5. Sur le configurer/propriétés de la connexion paginez, n'utilisez 8 bits de données, aucune parité, et 1 bit d'arrêt. Appelez les préférences pour l'utiliser sont **attente la tonalité avant la composition** et **pour annuler l'appel sinon connecté après 200 secondes**.
6. À la page de connexion, cliquez sur **avancé**. Dans les paramètres de connexion avancés, sélectionnez seulement le **contrôle de flux matériel** et le **type de modulation norme**. La page sur de configurer/options propriétés, rien devrait être cochée excepté la case sous le contrôle d'état.
7. Cliquez sur OK et puis cliquez sur Next.
8. Introduisez le numéro de téléphone de la destination, cliquez sur Next de nouveau, et cliquez sur Finish alors.
9. Une fois que la nouvelle icône de connexion apparaît, cliquez avec le bouton droit-la et choisissez Properties > **type de serveur**.
10. Choisissez le **PPP : Le WINDOWS 95, WINDOWS NT 3.5, Internet** et ne vérifie aucune option avancée.
11. **TCP/IP de** contrôle sous des protocoles réseau permis.
12. Sous des configurations TCP/IP..., choisissez le **serveur adresse IP assignée, serveur les adresses assignées de Serveur de noms**, et la **passerelle par défaut d'utilisation sur le réseau distant** et puis cliquez sur OK.
13. Quand l'utilisateur double-cliquer l'icône pour faire le connecter à l'affichage de fenêtre afin de composer, l'utilisateur doit compléter les champs de nom d'utilisateur et de mot de passe, et puis clique sur **se connectent**.

## Microsoft Windows a installé pour l'utilisateur 3

La configuration pour l'utilisateur 3 (utilisateur d'authentification avec le PPP d'autocommand) est identique que pour les utilisateurs 1 et 2 à ces exceptions :

- Page sur de configurer/options propriétés (étape 6), contrôle **apportent le terminal window après composition**.
- Quand l'utilisateur double-cliquer l'icône pour ouvrir le connecter à la fenêtre pour composer (étape 13), l'utilisateur ne complète pas les champs de nom d'utilisateur et de mot de passe. Les clics d'utilisateur **se connectent**. Après que le rapport au routeur soit établi, l'utilisateur

saisit le nom d'utilisateur et mot de passe dans la fenêtre noire qui apparaît. Après authentification, les presses d'utilisateur **continuent (F7)**.

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

### Routeur

Reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'émettre des commandes **debug**.

- **terminal monitor** — Les affichages **mettent au point des** messages d'erreur de sortie de commande et de système pour le terminal et la session en cours.
- **debug ppp negotiation** — Paquets PPP d'affichages envoyés pendant le startup de PPP, où des options PPP sont négociées.
- **paquet de debug ppp** — Affiche les paquets PPP qui sont envoyés et reçus. (Cette commande affiche des vidages mémoire de paquet à bas niveau.)
- **debug ppp chap** — Affiche des informations au sujet de si un client passe l'authentification (pour des versions du logiciel Cisco IOS plus tôt que 11.2).
- **debug aaa authentication** — Affiche des informations sur l'authentification de l'Authentification, autorisation et comptabilité (AAA) /TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.

### Serveur

**Note:** Ceci assume le code de serveur de logiciel gratuit TACACS+ de Cisco.

```
tac_plus_executable -C config.file -d 16  
tail -f /var/tmp/tac_plus.log
```

## Informations connexes

- [Page d'assistance TACACS+](#)
- [TACACS+ dans la documentation d'IOS](#)
- [Cisco Secure Access Control Server](#)
- [Configuration et débogage de CiscoSecure 2.x TACACS+](#)
- [Support et documentation techniques - Cisco Systems](#)