

Authentification pour l'administration HTTP sur AP version 1.01

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configuration ACS](#)

[Configuration d'interface](#)

[Configuration utilisateur](#)

[Configuration de groupe](#)

[Configuration du réseau](#)

[Configuration AP pour VxWorks](#)

[Configuration utilisateur](#)

[Configuration du serveur](#)

[Configuration AP pour l'IOS](#)

[Vérifier](#)

[Dépanner](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit une configuration d'échantillon pour l'authentification pour l'admin de HTTP sur la version 1.01 du Point d'accès (AP).

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.6.4 et ultérieures du serveur de contrôle d'accès (ACS)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Il n'y a aucune option de configurer l'autorisation TACACS+ ou de comptabilité ou de commande de RADIUS pour des sessions d'EXEC dans le GUI. Ces options peuvent être configurées dans le CLI, mais ne sont pas recommandées. Si vous configurez ces options, elles peuvent sévèrement s'embarber AP et l'ACS avec la comptabilité ou les demandes d'autorisation (chaque élément de chaque page doit être expliqué ou autorisé).

Configuration ACS

Configuration d'interface

Terminez-vous ces étapes pour configurer l'interface :

1. Dans TACACS+ (Cisco IOS), sélectionnez la case de groupe pour le premier nouveau champ éliminé de service.
2. Dans le domaine de service, entrez dans l'**Aironet**.
3. Dans le domaine de Protocol, écrivez le **shell**.
4. Dans les options de configuration avancée, choisissez les **caractéristiques avancées > l'affichage TACACS+ qu'une fenêtre pour chaque service a sélectionné**.
5. Cliquez sur **Submit**.

Configuration utilisateur

Terminez-vous ces étapes pour configurer l'utilisateur :

1. Dans les configurations avancées TACACS+, sélectionnez le **shell (exécutif)**.
2. Niveau de privilège choisi.
3. Dans le domaine, écrivez **15**.
4. Cliquez sur **Submit**.

Configuration de groupe

Terminez-vous ces étapes pour configurer le groupe :

1. Choisissez **TACACS+**.
2. Choisissez le **shell > les attributs personnalisés d'Aironet**.
3. Dans le domaine d'attributs personnalisés, entrez dans l'**Aironet : admin-**

`capability=write+ident+firmware+admin+snmp.`

4. Cliquez sur **Submit**.
5. Reprise.

Configuration du réseau

Terminez-vous ces étapes pour configurer le réseau :

1. Créez le NAS pour AP utilisant TACACS+ comme protocole.
2. La clé est le secret partagé d'AP.
3. Cliquez sur **Submit**.
4. Reprise.

Remarque: Si vous utilisez un serveur de jetons avec un mot de passe d'une fois, vous devez configurer la mise en antémémoire symbolique afin d'éviter d'être continuellement incitée pour des mots de passe du niveau 1 et du niveau 15. Terminez-vous ces étapes pour configurer la mise en cache symbolique :

1. Écrivez la configuration de groupe pour le groupe auquel vos utilisateurs d'admin appartiennent.
2. Choisissez les **configurations symboliques de carte**.
3. **Durée** choisie.
4. Choisissez une durée qui équilibre vos besoins de Sécurité et de commodité.

Si votre session typique d'admin dure cinq minutes ou moins, alors une valeur de durée de cinq minutes est la meilleure. Si votre session exécute plus long que cinq minutes, vous êtes incité de nouveau pour votre mot de passe à cinq intervalles minute. Notez que l'option de session ne fonctionne pas sans rendre compte activée. En outre, notez que la mise en cache symbolique est en vigueur pour *tous les* utilisateurs dans le groupe, et pour les sessions de *tout les* groupe avec tous les périphériques (pas simplement sessions d'EXEC à AP).

Configuration AP pour VxWorks

Configuration utilisateur

Procédez comme suit :

1. Choisissez l'installation > la **Sécurité** > les informations utilisateur > ajoutent le **nouvel utilisateur**.
2. Ajoutez un nouvel utilisateur avec de pleines capacités administratives (toutes les configurations de capacité vérifiées).
3. Clic **de retour**. Vous êtes retourné à la page de configuration de la sécurité.
4. **User Manager** de clic. La page d'User Manager Setup paraît.
5. **User Manager** d'enable.
6. Cliquez sur **OK**.

Configuration du serveur

Procédez comme suit :

1. Choisissez l'**installation > la Sécurité > le serveur d'authentification**.
2. Entrez dans l'adresse IP du serveur TACACS+.
3. Sélectionnez le type de serveur TACACS.
4. Dans le domaine, entrez dans le **port 49**.
5. Dans le domaine, écrivez le **secret partagé**.
6. Choisissez la case d'**authentification de l'utilisateur**.

[Configuration AP pour l'IOS](#)

Terminez-vous ces étapes pour configurer AP pour l'IOS :

1. Choisissez le **Security > Server Manager**.
2. Choisissez un serveur configuré TACACS+, ou configurez un neuf.
3. Cliquez sur **Apply**.
4. Choisissez l'IP du serveur TACACS+ dans le déroulant de l'authentification d'admin (TACACS+).
5. Cliquez sur **Apply**.
6. Choisissez la **Sécurité > l'admin Access**.
7. Créez un utilisateur local avec l'accès en lecture-écriture (si vous n'avez pas tellement déjà fait).
8. Cliquez sur **Apply**.
9. Choisissez le serveur d'authentification seulement ou le serveur d'authentification (sinon trouvé dans la liste locale).
10. Cliquez sur **Apply**.

[Vérifier](#)

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

[Dépanner](#)

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Support de produit de gamme 1200 d'Aironet](#)
- [Support technique de Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Support produit de Cisco Secure Access Control Server pour Windows](#)
- [Support produit de Cisco Secure Access Control Server pour Unix](#)
- [Support technique - Cisco Systems](#)