Guide de configuration d'EAP-TLS version 1.01

ID de document : 64064

Mis à jour : Oct. 14, 2009

 PDF de téléchargement

 Copie

Commentaires

Produits connexes

- Point d'accès Cisco Aironet 1200
- Points d'accès Cisco Aironet 350
- Cisco Secure Access Control Server pour Unix
- **Cisco Secure Access Control Server pour Windows**

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour la version 1.01 de Layer Security de Protocol-transport d'authentification extensible (EAP-TLS).

Remarque: Ce document suppose que vous utilisez Microsoft Certificate Authority (CA). Tandis que vous pouvez utiliser un certificat auto-signé, Cisco décourage fortement cette pratique, et ce document ne couvre pas les Certificats auto-signés. La période par défaut d'expiration des Certificats auto-signés est seulement un an, et vous ne pouvez pas changer cette configuration. C'est assez standard pour des Certificats de serveur. Cependant, le certificat auto-signé agit également en tant que certificat de CA de racine. Par conséquent, vous devez installer le nouveau certificat sur chaque client chaque année à moins que vous ne vérifiiez pas l'option « validiez de serveur certificat ». Un vrai CA doit être disponible pour obtenir les certificats client de toute façon, et ainsi, il n'y a vraiment aucune raison d'utiliser les Certificats auto-signés avec l'EAP-TLS.

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 :

- Point d'accès (AP) 12.02T1

- Serveur de contrôle d'accès (ACS) 3.1, 3.2, et 3.3
- Windows 2000 et XP
- Autorité de certification (CA) de racine d'entreprise

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 à Conventions relatives aux conseils techniques Cisco.

Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Installez le serveur du certificat de Microsoft (CA)

Procédez comme suit :

1. Choisissez le **début > les configurations > le panneau de configuration**.
2. Cliquez sur Add**/retirez les programmes au** panneau de configuration.
3. **Add/Remove Windows Components** choisi.
4. Sélectionnez les services de certificat.
5. Cliquez sur **Next** (Suivant).
6. Clic **oui au** message IIS.
7. Sélectionnez une racine autonome (ou entreprise) CA.
8. Cliquez sur **Next** (Suivant).
9. Nommez le CA.**Remarque:** Toutes les autres cases sont facultatives.**Remarque:** N'utilisez pas le même nom pour le CA que le serveur ACS, parce que ceci peut faire échouer les clients PEAP authentification. Un certificat de CA de racine avec la même chose nomment pendant que le certificat de serveur confond les clients PEAP. Ce problème n'est pas seul aux clients de Cisco. Naturellement, si vous ne prévoyez pas d'utiliser le PEAP, ceci ne s'applique pas.
10. Cliquez sur **Next** (Suivant).Le par défaut de base de données est correct.
11. Cliquez sur **Next** (Suivant).IIS doit être installé avant que vous installiez le CA.

Créez un certificat de serveur

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) de** votre serveur ACS.
2. Cochez la **demande une** case de **certificat**.

3. Cliquez sur **Next** (Suivant).
4. **Demande avancée** choisie.
5. Cliquez sur **Next** (Suivant).
6. Choisi **soumettez une demande de certificat à ce CA utilisant une forme**.
7. Cliquez sur **Next** (Suivant).
8. Introduisez un nom dans la case du nom (NC).
9. Cochez la case de **certificat d'authentification de serveur** pour le but visé.**Remarque:** Si vous utilisez l'entreprise CA, **serveur Web** choisi sur la première liste.
10. Sélectionnez ces options sous l'option principale de créer un nouveau modèle :**CSP — Microsoft Base Cryptographic Provider v1.0Taille de clé — 1024Remarque:** Les Certificats créés avec une taille de clé plus grande que 1024 peuvent fonctionner pour HTTPS mais pas pour le PEAP.**Remarque:** L'entreprise CA de Windows 2003 permet des tailles de clé plus grandes que 1024, mais un principal plus en grande partie que 1024 ne fonctionne pas avec le PEAP. L'authentification peut sembler passer dans ACS, mais le client s'arrête juste à la tentative d'authentification.Vérifiez les **clés de marque en tant qu'**option **exportableRemarque:** Microsoft a changé le modèle de serveur Web avec la release de l'entreprise CA de Windows 2003. Avec cette modification de modèle, vous pouvez plus n'exporter des clés, et l'option est greyed. Il n'y a aucun autre modèle de certificat fourni avec des services de certificat qui sont pour l'authentification de serveur, ou qui donnent la capacité de marquer des clés comme exportables. Afin de créer un nouveau modèle qui fait ainsi, voir la création par nouvelle section de modèle de certificat.Vérifiez l'option de **mémoire d'ordinateur local d'utilisationRemarque:** Retenez les sélections par défaut pour toutes autres options.
11. Cliquez sur **Submit**.Vous devez recevoir ce message : **Votre demande de certificat a été reçue**.

Créez un nouveau modèle de certificat

Procédez comme suit :

1. Choisissez **Start > Run**.
2. Tapez **certtmpl.msc dans la** boîte de dialogue de passage, et l'appuyez sur ENTRENT.
3. Cliquez avec le bouton droit le **modèle de serveur Web**, et sélectionnez le **modèle en double**.
4. Nommez le modèle, par exemple, ACS.
5. Sélectionnez l'onglet de **manipulation de demande**.
6. Vérifiez la **clé privée d'autoriser pour être** option **exportée**.
7. Sélectionnez le bouton de **CSPs**.
8. Vérifiez l'option de **Microsoft Base Cryptographic Provider v1.0**.
9. Cliquez sur **OK**.**Remarque:** Retenez les sélections par défaut pour toutes autres options.
10. Cliquez sur **Apply**.
11. Cliquez sur **OK**.
12. Ouvrez le CA MMC SNAP-dans.
13. Cliquez avec le bouton droit les **modèles de certificat**, et choisissez **nouveau > modèle de certificat à émettre**.
14. Choisissez le nouveau modèle que vous avez créé.
15. Cliquez sur **OK**.
16. Redémarrez le CA.Le nouveau modèle est inclus dans la liste de modèle de certificat.

Parfois, « `n'a pas créé « l'`erreur de `» objet » CertificateAuthority.Request` se produit quand

vous tentez de créer un nouveau certificat.

Terminez-vous ces étapes afin de corriger cette erreur :

1. Choisissez le **début > les outils d'administration > l'IIS**.
2. Développez les **sites Web > le site Web de par défaut**.
3. Cliquez avec le bouton droit **CertSrv**, et choisissez Properties.
4. Cliquez sur le **bouton configuration** dans la section de configurations d'application de l'onglet de répertoire virtuel.
5. Sélectionnez l'onglet d'**options**.
6. Vérifiez l'option d'**état de session d'enable**.**Remarque:** Retenez les sélections par défaut pour toutes autres options.
7. Cliquez deux fois sur **OK**.
8. Reprise IIS.**Remarque:** Des 2003 CA dans un domaine 2000 dont le schéma n'a pas été préparé pour la compatibilité 2003 avec adprep/forestprep/domainprep ne fonctionne pas avec l'EAP. Si votre navigateur verrouille avec un message « de `contrôle ActiveX de téléchargement` », vous devez exécuter la difficulté dans cet URL : http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B330389 .**Remarque:** Si le champ CSP affiche juste le « `chargement….` » assurez-vous que vous n'avez pas un pare-feu logiciel sur l'ordinateur qui soumet la demande. Le ZoneAlarm de ZoneLabs entraîne cette erreur à peu près chaque fois. Certain autre logiciel peut également entraîner cette erreur.

Approuvez le certificat du CA

Procédez comme suit :

1. Choisissez le **Start > Programs > Administrative tools > l'autorité de certification**.
2. Développez le certificat sur le volet gauche.
3. Choisi **en attendant des demandes**.
4. Clic droit sur le certificat.
5. Sélectionnez toutes les tâches.
6. **Question** choisie.

Installez le certificat sur des Windows Server

Téléchargez le certificat de serveur au serveur ACS

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) de** votre serveur ACS.
2. Sélectionnez le **contrôle sur un certificat en attente**.
3. Cliquez sur **Next** (Suivant).
4. Sélectionnez le certificat.
5. Cliquez sur **Next** (Suivant).
6. Cliquez sur **Install**.

Installez le certificat de CA sur le serveur ACS

Remarque: Ces étapes ne sont pas nécessaires si ACS et le CA sont installés sur le même serveur.

1. Procédez comme suit :

2. De votre serveur ACS, parcourez au CA (**http://IP_of_CA_server/certsrv/**).
3. Choisi **récupérez le certificat de CA ou la liste des révocations de certificat**.
4. Cliquez sur **Next** (Suivant).
5. **Base** choisie **64 encodée**.
6. Cliquez sur **Download CA certificate**.
7. Cliquez sur **Open**.
8. Le clic **installent le certificat**.
9. Cliquez sur **Next** (Suivant).
10. **Endroit** choisi **tous les Certificats dans la mémoire suivante**.
11. Cliquez sur **Browse**.
12. Cochez la case **physique de mémoires d'exposition**.
13. Développez la liste d'**Autorités de certification racine approuvée**.
14. Ordinateur local choisi.
15. Cliquez sur **OK**.
16. Cliquez sur **Next** (Suivant).
17. Cliquez sur **Finish** (Terminer).Une zone de message apparaît.
18. Cliquez sur **OK**.**Remarque:** Si vos certificats client étaient créés par un CA différent de votre certificat de serveur, vous devez répéter ces étapes pour la racine CA et n'importe quelle intermédiaire CAs impliquée dans la création de certificat client.

Installation ACS pour utiliser le certificat de serveur

Procédez comme suit :

1. **Configuration système de** clic sur le serveur ACS.
2. **Installation** choisie de **certificat ACS**.
3. Choisi **installez le certificat ACS**.
4. **Certificat** choisi d'**utilisation de mémoire**.
5. Introduisez dedans le nom NC (le même nom que vous avez tapé dans l'étape 8 de la création par section de certificat de serveur).
6. Cliquez sur **Submit**.
7. **Configuration de système de** clic sur le serveur ACS.
8. **Installation** choisie de **certificat ACS**.
9. Choisi **éditez la liste de confiance de certificat**.
10. Cochez la case **CA**.
11. Cliquez sur **Submit**.

Créez une demande de signature de certificat

Procédez comme suit :

1. Allez à la **configuration système > au certificat ACS installés > génèrent la demande de signature de certificat**.

2. Introduisez un nom dans le domaine de certificat dans le format de `cn=name`.
3. Introduisez un nom pour le fichier principal privé.**Remarque:** Ce champ cache le chemin à la clé privée. Par conséquent, si vous cliquez sur Submit une deuxième fois après que le CSR soit créé, la clé privée est remplacée, et n'appariera pas le CSR d'original. Ceci peut avoir comme conséquence « la `clé privée n'apparie pas` » l'erreur quand vous tentez d'installer le certificat de serveur.
4. Tapez le mot de passe de clé privée.
5. Confirmez le mot de passe.
6. Choisissez une longueur principale de 1024.**Remarque:** ACS peut générer des tailles de clé plus grandes que 1024. Cependant, un principal plus en grande partie que 1024 ne fonctionne pas avec l'EAP. L'authentification peut sembler passer dans ACS, mais le client s'arrête juste à la tentative d'authentification.
7. Cliquez sur **Submit**.
8. Copiez la sortie CSR du côté droit pour soumettre au CA.

Employez votre CSR pour créer un certificat de serveur

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) de** votre ftp server.
2. Sélectionnez la **demande une** option de **certificat**.
3. Cliquez sur **Next** (Suivant).
4. **Demande avancée** choisie.
5. Cliquez sur **Next** (Suivant).
6. Choisi **soumettez une demande de certificat utilisant un fichier PKCS encodé par base64 #10 ou une demande de renouvellement utilisant un fichier PKCS encodé par base64 #7**.
7. Collez la sortie de l'étape 8 de la création par section de demande de signature de certificat dans le champ encodé par Base64 de demande de certificat.
8. Cliquez sur **Submit**.
9. Cliquez sur **Download CA certificate**.
10. Cliquez sur la **sauvegarde**, introduisez un nom pour le certificat, et sauvegardez-le à votre répertoire de FTP.

Installez le certificat sur une appliance de Windows

Certificat de CA de téléchargement à votre ftp server

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) de** votre ftp server.
2. Choisi **récupérez le certificat de CA ou la liste des révocations de certificat**.
3. Cliquez sur **Next** (Suivant).
4. **Base** choisie **64 encodée**.
5. Cliquez sur **Download CA certificate**.
6. Cliquez sur la **sauvegarde**, introduisez un nom pour le certificat, et sauvegardez-le à votre répertoire de FTP.

Installez le certificat de CA sur votre appliance

Procédez comme suit :

1. Allez à la **configuration système > au certificat ACS installés > installation d'autorité de certification ACS**.
2. Cliquez sur Download le **fichier de certificat de CA**.
3. Tapez l'adresse IP ou l'adresse Internet du ftp server dans le domaine serveur ftp.
4. Tapez un nom d'utilisateur valide que le Cisco Secure ACS peut employer pour accéder au ftp server dans le domaine de procédure de connexion.
5. Tapez le mot de passe correct pour le nom d'utilisateur dans le domaine de mot de passe.
6. Tapez le chemin relatif à partir du répertoire racine serveur ftp au répertoire qui contient le fichier de certificat de CA dans le domaine distant de répertoire de FTP.
7. Introduisez le nom du fichier de certificat de CA dans le domaine distant de nom du fichier de FTP.
8. Cliquez sur **Submit**.
9. Vérifiez le nom du fichier dans le domaine.
10. Cliquez sur **Submit**.
11. Redémarrez les services ACS dans la **configuration système > le contrôle des services**.**Remarque:** Si vous ignorez les étapes dans le certificat de CA de téléchargement à votre ftp server et les installez le certificat de CA sur vos sections une d'appareils de ces deux situations peut surgir :Vous ne pouvez pas activer l'EAP-TLS, et un message d'erreur semble déclarer que le certificat de serveur n'est pas installé quoique le certificat soit installé.Alternativement, la panne `non configurée de type d'EAP` se produit dans les essais ratés quoique le type d'EAP soit configuré.**Remarque:** Notez également que, si vous utilisiez une intermédiaire CA pour créer votre certificat de serveur, vous devez répéter ces étapes pour chaque CA dans la chaîne entre la racine CA et le certificat de serveur (certificat de CA y compris de racine). Supplémentaire, si vous créiez vos certificats client par un CA différent de votre certificat de serveur, vous devez répéter ces étapes pour la racine CA et n'importe quelle intermédiaire CAs impliquée dans la création de certificat client.

Installez le certificat de serveur sur votre appliance

Procédez comme suit :

1. Allez à l'**installation de configuration système > de certificat ACS**.
2. Le clic **installent le certificat ACS**.
3. Sélectionnez le certificat lu de l'option de fichier.
4. Cliquez sur le lien de **fichier du certificat de téléchargement**.
5. Tapez l'adresse IP ou l'adresse Internet du ftp server dans le domaine serveur ftp.
6. Tapez un nom d'utilisateur valide que le Cisco Secure ACS peut employer pour accéder au ftp server dans le domaine de procédure de connexion.
7. Tapez le mot de passe correct dans le domaine de mot de passe.
8. Tapez le chemin relatif à partir du répertoire racine serveur ftp au répertoire qui contient le fichier du certificat de serveur dans le domaine distant de répertoire de FTP.
9. Introduisez le nom du fichier du certificat de serveur dans le domaine distant de nom du fichier de FTP.

10. Cliquez sur **Submit**.
11. Tapez le chemin et le mot de passe pour la clé privée. Référez-vous aux étapes 3 et 4 de la création par section de demande de signature de certificat.
12. Cliquez sur **Submit**.

Autre tâches

Configurez les configurations globales d'authentification

Procédez comme suit :

1. **Configuration système de** clic sur le serveur ACS.
2. **Installation globale d'authentification de** clic.
3. Le contrôle **permettent l'EAP-TLS**.
4. Sélectionnez un ou plusieurs options de vérification de certificat. Si vous sélectionnez toutes les méthodes, ACS essaye chaque méthode dans l'ordre jusqu'à ce qu'une vérification réussie se produise ou jusqu'à la dernière méthode échoue.
5. Cliquez sur **Submit**.
6. Redémarrez le PC.

Installez AP sur l'ACS

Terminez-vous ces étapes pour installer AP sur l'ACS :

1. Cliquez sur Network Configuration sur le serveur ACS.
2. Cliquez sur Add l'**entrée** afin d'ajouter un client d'AAA.
3. Spécifiez ces valeurs dans les cases :Adresse IP de client d'AAA — IP_of_your_APClé — Composez un principal (assurez-vous que la clé apparie la clé secrète partagée par AP)Authentifiez utilisant — RAYON (Cisco Aironet)
4. Cliquez sur **Submit**.
5. Redémarrez le PC.**Remarque:** Ne changez pas les par défaut l'uns des sur l'installation de client d'AAA.

Configurez AP

Remarque: Le réseau-EAP est nécessaire si vous voulez installer l'ACU.

Si vous utilisez la rotation principale d'émission, vous n'avez pas besoin de placer une clé pendant que la clé doit déjà être placée. Si la clé n'est pas placée, allez **installer > avance de radio** et placer une valeur pour la rotation de clé d'émission. Vous n'avez pas besoin probablement de placer ceci puis des 5 minutes inférieures (300 sec). Après que vous placiez la valeur, cliquez sur OK, et revenez à la page par radio de chiffrement de données.

VxWorks

Procédez comme suit :

1. Ouvrez AP.

2. Choisissez l'**installation > la Sécurité > le serveur d'authentification**.
3. Écrivez l'adresse IP ACS.
4. Écrivez le secret partagé. Cette valeur doit apparier la clé ACS.
5. Cochez la case d'**authentification EAP**.
6. Cliquez sur **OK**.
7. Choisissez l'**installation > la Sécurité > le chiffrement de données de radio**.
8. Cochez la case **ouverte**.
9. Si vous n'utilisez pas la rotation principale d'émission, la **clé WEP** choisie **1** et **128**.
10. Changez l'utilisation du chiffrement de données par des stations au **chiffrement complet** (si vous ne pouvez pas changer ceci, cliquez sur Apply d'abord).
11. Cliquez sur **OK**.

Interface web IOS AP

Procédez comme suit :

1. Choisissez le **Security > Server Manager**.
2. Choisissez le RAYON de la liste en cours de serveur.
3. Tapez l'adresse IP ACS.
4. Tapez le secret partagé. Cette valeur doit apparier la clé dans ACS.
5. Cochez la case d'**authentification EAP**.
6. De la liste d'authentification EAP, choisissez l'adresse IP du serveur de RAYON.
7. Cliquez sur OK sur la boîte de dialogue d'avertissement.
8. Cliquez sur **Apply**.

Gestionnaire SSID (cryptage WEP seulement)

Terminez-vous ces étapes pour le cryptage WEP seulement :

1. Choisissez le SSID de la liste du courant SSID, ou spécifiez un nouveau SSID dans le champ SSID.
2. Cochez la case **ouverte d'authentification**.
3. Choisissez **avec l'EAP de la** liste.
4. Cochez la case d'**EAP de réseau**.
5. Cliquez sur **Apply**.

Gestionnaire de cryptage (cryptage WEP seulement)

Terminez-vous ces étapes pour le cryptage WEP seulement :

1. Choisissez **Security > Encryption Manager**.
2. Cliquez sur la case d'option de **cryptage WEP**.
3. Choisissez obligatoire de la liste.
4. Cliquez sur la case d'option de la **clé de chiffrement 1**.
5. Spécifiez la clé.
6. Choisissez **128 de la** liste de taille de clé.
7. Cliquez sur **Apply**.**Remarque:** La configuration diffère si vous utilisez le WPA. Voir l'annexe de Gestion de clé WPA à la fin de ce document pour des détails.

Téléchargez et installez le certificat de CA de racine pour le client

Cette étape *est exigée* pour *chaque* client pour que l'EAP-TLS travaille à ce client. Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) du** PC client.
2. Choisi **récupérez un certificat de CA**.
3. Cliquez sur **Next** (Suivant).
4. **Base** choisie **64 encodée**.
5. Cliquez sur **Download CA certificate**.
6. Cliquez sur **Open**.
7. Cliquez sur **Install Certificate**.
8. Cliquez sur **Next** (Suivant).
9. **Endroit** choisi **tous les Certificats dans la mémoire suivante**.
10. Cliquez sur **Browse**.
11. Cochez la case **physique de mémoires d'exposition**.
12. Développez les **Autorités de certification racine approuvée**, et sélectionnez l'**ordinateur local**.
13. Cliquez sur **OK**.
14. Cliquez sur **Next** (Suivant).
15. Cliquez sur **Finish** (Terminer).
16. Cliquez sur OK sur la zone de message avec l'`importation était` message `réussi`.

Créez le certificat client

Entreprise CA

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) du** compte utilisateur du client.
2. Sélectionnez la **demande une** option de **certificat**.
3. Cliquez sur **Next** (Suivant).
4. **Demande avancée** choisie.
5. Cliquez sur **Next** (Suivant).
6. Choisi **soumettez une demande de certificat à ce CA utilisant une forme**.
7. Cliquez sur **Next** (Suivant).
8. Choisissez l'**utilisateur** dans la liste de modèle de certificat.
9. Placez ces valeurs sous les options principales :CSP — Microsoft Base Cryptographic Provider v1.0Taille de clé — 1024Toutes autres options — Retenez les valeurs par défaut
10. Cliquez sur **Submit**.Une zone de message apparaît avec la `votre demande de certificat a été…` message `reçu`.

CA autonome

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) du** compte utilisateur du client.
2. Sélectionnez la **demande une** option de **certificat**.

3. Cliquez sur **Next** (Suivant).
4. **Demande avancée** choisie.
5. Cliquez sur **Next** (Suivant).
6. Choisi **soumettez une demande de certificat à ce CA utilisant une forme**.
7. Cliquez sur **Next** (Suivant).
8. Tapez le nom d'utilisateur dans le domaine NC. Cette valeur doit apparier le nom d'utilisateur dans la base de données d'authentification.
9. Certificat choisi d'authentification client pour le but visé.
10. Placez ces valeurs sous les options principales :CSP — Microsoft Base Cryptographic Provider v1.0Taille de clé — 1024Toutes autres options — Retenez les valeurs par défaut
11. Cliquez sur **Submit**.Une zone de message apparaît avec la `votre demande de certificat a été…` message `reçu`.

Approuvez le certificat client du CA

Procédez comme suit :

1. Choisissez le **Start > Programs > Administrative tools > l'autorité de certification** pour ouvrir le CA.
2. Développez le certificat du côté gauche.
3. **Demandes en attendant de** clic.
4. Cliquez avec le bouton droit sur le certificat et sélectionnez toutes les tâches.
5. **Question** choisie.

Installez le certificat client sur le PC client

Procédez comme suit :

1. Parcourez au CA (**http://IP_of_CA_server/certsrv/) du** compte utilisateur du client.
2. Sélectionnez le **contrôle sur un certificat en attente**.
3. Cliquez sur **Next** (Suivant).
4. Sélectionnez le certificat.
5. Cliquez sur **Next** (Suivant).
6. Cliquez sur **Install**.**Remarque:** Afin de vérifier l'installation de certificat, allez à Microsoft Internet Explorer, et sélectionnez les **outils > les options Internet > le contenu > les Certificats**. Un certificat avec le nom de l'user-id ou du nom d'utilisateur ouvert une session doit être présent.

Faites confiance au certificat client sur ACS

Vous devez exécuter ces étapes seulement si les certificats client et le certificat de serveur étaient créés par le CAs différent.

1. Assurez-vous que le certificat de CA de racine et les Certificats CA intermédiaires ont été installés selon les étapes dans l'installer le certificat de CA sur le serveur ACS et installez le certificat de CA sur vos sections d'appareils.
2. Allez à la **configuration système > au certificat ACS installés** sur l'ACS.
3. Cliquez sur Edit la **liste de confiance de certificat**.

4. Cochez la case à côté de la racine CA qui a créé le certificat client.
5. Cliquez sur **Submit**.

Installez le client pour l'EAP-TLS

Procédez comme suit :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**.
2. Cliquez avec le bouton droit le réseau Sans fil, et sélectionnez **Properties**.
3. Cliquez sur l'onglet de **réseau sans fil**.
4. Assurez-vous que des **fenêtres d'utilisation à configurer…** est vérifiées.
5. Cliquez sur Configure si vous voyez le SSID dans la liste. Sinon, cliquez sur Add.
6. Mettez dans le SSID.
7. Vérifiez le **WEP** et la **clé est donné pour moi automatiquement des** cases.
8. Sélectionnez l'onglet d'**authentification**.**Remarque:** Si vous ne voyez pas l'onglet d'authentification, le service de 802.1X est installé dans un état handicapé. Afin de résoudre ce problème, vous devez activer le service de configuration Sans fil dans la liste des services. Procédez comme suit :Cliquez avec le bouton droit **mon ordinateur**, et choisi **gérez**.**Services et applications de** clic.**Services de** clic.Placez la valeur de démarrage pour le service à **automatique**.Commencez le service.**Remarque:** Si l'onglet d'authentification est présent mais est indisponible, ceci indique que le gestionnaire d'adaptateur réseau ne prend en charge pas le 802.1x correctement. Référez-vous en utilisant l'authentification de 802.1x sur les ordinateurs client qui sont Windows 2000 courant .
9. Assurez-vous que le **contrôle d'accès au réseau d'enable utilisant…** est vérifié.
10. **Smart Card** choisi **ou tout autre certificat** pour le type d'EAP, et clic **Properties**.
11. Sélectionnez le **certificat d'utilisation en cette** option d'**ordinateur**.
12. Cochez la case **simple de sélection de certificat d'utilisation**.
13. Cochez la case pour le CA sous le certificat racine de confiance.
14. Cliquez sur OK trois fois.

Annexe d'authentification de machine

L'authentification de machine d'EAP-TLS *exige le* Répertoire actif et une racine CA d'entreprise afin de saisir un certificat pour l'authentification de machine d'EAP-TLS, l'ordinateur doit avoir la Connectivité à l'entreprise CA par une connexion câblée ou par la connexion Sans fil avec la Sécurité de 802.1x désactivée. C'est la *seule* manière d'obtenir un certificat valide d'ordinateur (avec « ordinateur » dans le gisement « de modèle de certificat »). Une fois terminé, le certificat d'ordinateur est installé dans les **Certificats (ordinateur local) > personnel >** répertoire de **Certificats** une fois visualisé dans les Certificats (ordinateur local) MMC SNAP-dans. Le certificat contient entièrement - le nom d'ordinateur qualifié d'AD dans le sujet et des domaines SAN. Un certificat qui soutient le nom de l'ordinateur mais n'a pas été créé comme décrit dans cette section n'est pas un véritable certificat d'ordinateur (avec le « ordinateur » dans le domaine de modèle de certificat). Un tel certificat n'est pas utilisé pour l'authentification de machine mais plutôt le SYSTÈME D'EXPLOITATION voit un certificat tel qu'un certificat utilisateur normal.

Installation ACS pour permettre l'authentification de machine

Procédez comme suit :

1. Allez aux **bases de données d'utilisateur externe > à la configuration de base de données**.
2. **Base de données de Windows de** clic.
3. Cliquez sur **Configure**.
4. Cochez la case d'**authentification de machine d'EAP-TLS d'enable**.
5. Cliquez sur **Submit**.

Configurez le domaine pour l'Auto-inscription de certificat

Procédez comme suit :

1. Ouvrez les utilisateurs et les ordinateurs MMC SNAP-dans en fonction un contrôleur de domaine.
2. Cliquez avec le bouton droit l'entrée de domaine et sélectionnez **Properties**.
3. Allez à l'onglet de **stratégie de groupe**.
4. sélectionnez la **stratégie par défaut de domaine**.
5. Cliquez sur **Edit**.
6. Allez à la **configuration de l'ordinateur > aux paramètres de windows > aux paramètres de sécurité > des stratégies de clé publique**.
7. **Configurations automatiques de demande de certificat de** clic droit.
8. Choisissez la **nouvelle > automatique demande de certificat**.
9. Cliquez sur **Next** (Suivant).
10. **Ordinateur de** point culminant.
11. Cliquez sur **Next** (Suivant).
12. Vérifiez l'entreprise CA.
13. Cliquez sur **Next** (Suivant).
14. Cliquez sur **Finish** (Terminer).

Installez le client pour l'authentification de machine

Joignez le domaine

Si le client joignait le domaine avant que vous ayez configuré l'Auto-inscription, le certificat doit être fourni à l'ordinateur la prochaine fois que vous redémarrez l'ordinateur après l'Auto-inscription est configurée sans nécessité re-de joindre l'ordinateur au domaine.

Terminez-vous ces étapes pour joindre le domaine :

1. Connectez-vous dans Windows avec un compte qui a des privilèges d'administrateur.
2. Cliquez avec le bouton droit sur **mon ordinateur** et choisissez Properties.
3. Sélectionnez l'onglet de **nom de l'ordinateur**.
4. Cliquez sur **Change**.
5. Tapez le nom d'hôte dans le domaine de nom de l'ordinateur.
6. **Domaine** choisi.
7. Introduisez le nom du domaine.
8. Cliquez sur **OK**.Une boîte de dialogue de connexion apparaît.
9. Ouvrez une session avec des qualifications d'un compte qui a l'autorisation de joindre le domaine.L'ordinateur joint le domaine.
10. Redémarrez l'ordinateur.L'ordinateur est maintenant un membre du domaine, et a un

certificat pour le CA et un certificat d'ordinateur installé.

Suppliant d'EAP-TLS d'installation pour l'authentification de machine

Procédez comme suit :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**.
2. Cliquez avec le bouton droit la connexion réseau et sélectionnez **Properties**.
3. Sélectionnez l'onglet d'**authentification**.
4. Le contrôle **authentifient comme ordinateur**.

Annexe de Gestion de clé WPA

Cette section s'applique au Cisco IOS AP 12.02(13)JA1, ACS 3.2, et XP SP1 avec le correctif WPA. Selon la documentation dans cette section, les clients de Windows 2000 ne prennent en charge pas à la façon des indigènes la Gestion de clé WPA et vous devez employer le logiciel client du constructeur afin d'obtenir ce support. Référez-vous à l'aperçu de la mise à jour de sécurité Sans fil WPA dans Windows XP .

L'ACU de Cisco ne prend en charge pas la Gestion de clé WPA pour l'EAP géré par le système central (EAP-TLS et PEAP) actuellement. Vous devez installer un tiers client, par exemple, le client d'odyssée de trouille ou le client d'ÉGIDE de temple. Référez-vous aux documents d'adaptateur LAN sans fil pour Windows pour plus d'informations sur le soutien WPA des Produits Cisco. Ces informations s'appliquent aux clients du Windows Mobile 2003 (PC de poche) également.

La Gestion de clé WPA est fondamentalement identique, mais diffère dans ces deux procédures :

1. Configurez AP.
2. Installez le client de XP pour l'EAP-TLS et le WPA.

Configurez AP

Procédez comme suit :

1. Allez au **Security > Encryption Manager**.
2. Cliquez sur l'option de **chiffrement WEP**.
3. Choisissez le **TKIP**.
4. Cliquez sur **Apply**.
5. Allez au **Security > SSID Manager**.
6. Choisissez le SSID de la liste du courant SSID. Alternativement, vous pouvez spécifier un nouveau SSID dans le champ SSID.
7. **Authentification ouverte de** contrôle.
8. Choisissez **avec l'EAP de la** liste.
9. **EAP de réseau de** contrôle.
10. **Obligatoire** choisi de la liste sous l'Authenticated Key Management.
11. Clic **WPA**.
12. Cliquez sur **Apply**.

Installez le client de XP pour l'EAP-TLS et le WPA

Procédez comme suit :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**.
2. Cliquez avec le bouton droit le réseau Sans fil, et sélectionnez **Properties**.
3. Sélectionnez l'onglet de **réseau sans fil**.
4. Assurez-vous que les **fenêtres d'utilisation pour configurer l'**option est vérifiées.
5. Cliquez sur Configure si vous voyez le SSID dans la liste. Sinon, cliquez sur Add.
6. Mettez dans le SSID.
7. Choisissez le **WPA** pour l'authentification de réseau.
8. Choisissez le **TKIP** pour le chiffrement de données.
9. Sélectionnez l'onglet d'**authentification**.
10. Assurez-vous que l'**utilisation de contrôle d'accès au réseau d'enable** est vérifiée.
11. **Smart Card** choisi **ou tout autre certificat** pour le type d'EAP.
12. Cliquez sur **Properties**.
13. Sélectionnez le **certificat d'utilisation en cette** option d'**ordinateur**.
14. Cochez la case **simple de sélection de certificat d'utilisation**.
15. Cochez la case pour le CA sous le certificat racine de confiance.
16. Cliquez sur OK trois fois.

Vérifiez

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

Dépannez

Erreur : Problème avec le certificat tout en se connectant au WLAN

Cette erreur apparaît sur le client sans fil.

```
Le serveur « server> de <Authentication » a présenté un certificat valide délivré par le « name>
<CA », mais le « name> <CA » n'est pas configuré car une ancre valide de confiance pour ce
profil.
```

Solution

Afin de résoudre ce problème, vous pouvez exporter le certificat racine du CA qui a fourni le certificat au serveur d'authentification à un fichier. Copiez le fichier sur le client sans fil et puis exécutez cette commande d'une invite de commande élevée.

```
certutil - entreprise - addstore NTAuth CA_CertFilename.cer
```

Référez-vous à l'alerte de protection windows apparaît en se connectant à un réseau Sans fil sur un pour en savoir plus d'ordinateur de groupe de travail.

Informations connexes

- Cisco Secure ACS pour la page d'assistance de Windows
- Cisco Secure ACS pour la page de support UNIX
- Support et documentation techniques - Cisco Systems

Ce document était-il utile ? Oui aucun

Merci de votre feedback.

Ouvrez une valise de support (exige un contrat de service Cisco.)

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Oct. 14, 2009
ID de document : 64064